Planificación y conceptos del plano de control de IaaS de vSpere

Actualización 3
VMware vSphere 8.0
VMware vCenter 8.0
VMware ESXi 8.0



Puede encontrar la documentación técnica más actualizada en el sitio web de VMware by Broadcom en:

https://docs.vmware.com/es/

VMware by Broadcom
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contenido

Planificación y conceptos del plano de control de IaaS de vSphere

La guía *Planificación y conceptos del plano de control de IaaS de vSphere* proporciona información sobre los principales conceptos y la arquitectura de vSphere IaaS control plane, conocido formalmente como vSphere with Tanzu, así como los requisitos que debe cumplir el entorno de vSphere para que se pueda habilitar vSphere IaaS control plane en los clústeres de vSphere y para ejecutar cargas de trabajo en clústeres de Tanzu Kubernetes Grid, pods de vSphere y máquinas virtuales creadas con el servicio de VM.

Audiencia prevista

Esta información está destinada a los administradores de vSphere y los ingenieros de desarrollo y operaciones que desean familiarizarse con los requisitos para habilitar vSphere IaaS control plane en vSphere y los principales conceptos y la arquitectura de la plataforma.

Información actualizada

Esta documentación sobre *Planificación y conceptos del plano de control de IaaS de vSphere* se actualiza con cada versión del producto o cuando sea necesario.

En esta tabla se muestra el historial de actualizaciones de *Planificación y conceptos del plano de control de IaaS de vSphere*.

Revisión	Descripción
18 de abril de 2024	Se actualizó la información de licencias para las nuevas licencias de la solución. Consulte Licencias para vSphere IaaS control plane.
29 de febrero de 2024	Se ha agregado contenido para las nubes. Consulte Componentes de NSX Advanced Load Balancer.
07 de febrero de 2024	Se ha actualizado un enlace en Redes del Supervisor.
13 DEC 2023	Se han actualizado los requisitos de NSX con una nota sobre la preparación de todos los hosts ESXi que participan en el clúster de vSphere como nodos de transporte de NSX. Consulte Requisitos para Supervisor zonal con NSX y Requisitos para la implementación de clústeres de Supervisor con NSX.
29 de septiembre de 2023	Se han actualizado los requisitos del equilibrador de carga para implementar HAProxy. Consulte Requisitos para la implementación de un Supervisor zonal con equilibrador de carga de HAProxy y Requisitos para la implementación de clústeres de Supervisor con redes VDS y equilibrador de carga de HAProxy
21 de septiembre de 2023	Se agregó contenido para las redes de Supervisor con NSX y NSX Advanced Load Balancer. Consulte Flujos de trabajo y funciones de usuario de vSphere IaaS control plane y Redes del Supervisor.
3 de agosto de 2023	Revisiones menores.
30 de junio de 2023	■ Se agregó una declaración sobre la distribución de las zonas de vSphere en las citas físicas: Implementaciones de clúster y de Supervisor zonal
9 de junio de 2023	■ Se agregó la siguiente declaración a Seguridad de vSphere IaaS control plane: El mismo modelo de cifrado se aplica a los datos de la base de datos (etcd) que está instalada en el plano de control de cada clúster de Tanzu Kubernetes Grid. ■ Se agregó una declaración donde se indica que Storage vMotion no es compatible con los volúmenes persistentes. Consulte Cómo se integra Supervisor con el almacenamiento de vSphere y Almacenamiento para clústeres de Tanzu Kubernetes Grid. ■ Se agregó una recomendación para separar los dominios de administración y de carga de trabajo como práctica recomendada en Capítulo 5 Requisitos para la implementación de Supervisor zonal y Capítulo 6 Requisitos para la implementación de clústeres de Supervisor.
2 de junio de 2023	■ Se agregó un vínculo a la Guía de diseño de referencia de NSX. Consulte Requisitos para Supervisor zonal con NSX y Requisitos para la implementación de clústeres de Supervisor con NSX. ■ Actualizaciones menores.

Revisión	Descripción
30 de mayo de 2023	■ Se agregó el requisito de compatibilidad de la encapsulación GENEVE para las implementaciones de NSX. Consulte Requisitos para el supervisor zonal con NSX y Requisitos para la implementación del clúster supervisor con NSX. ■ Actualizaciones menores.
12 de mayo de 2023	Se agregó una nota para indicar que si actualizó el entorno de vSphere IaaS control plane desde una versión de vSphere anterior a la versión 8.0 y desea utilizar zonas de vSphere, debe crear un nuevo Supervisor de tres zonas. Consulte Capítulo 5 Requisitos para la implementación de Supervisor zonal.
9 de mayo de 2023	■ Se agregó un tema independiente sobre ¿Qué es un espacio de nombres de vSphere?. ■ Se actualizó el contenido sobre Gestión de identidad y acceso de vSphere IaaS control plane. ■ Se agregó una nota que indica que los pods de vSphere solo se admiten con la pila de redes NSX. Consulte ¿Qué es un pod de vSphere?.
1 de mayo de 2023	Revisiones menores.
18 de abril de 2023	Actualizaciones generales de la versión de vSphere 8 Update 1.

Conceptos de vSphere IaaS control plane

1

Mediante el uso de vSphere IaaS control plane, puede convertir los clústeres de vSphere en una plataforma para ejecutar las cargas de trabajo de Kubernetes en grupos de recursos dedicados en vSphere. Una vez que está habilitado en los clústeres de vSphere, vSphere IaaS control plane crea un plano de control de Kubernetes directamente en la capa de hipervisor. A continuación, puede ejecutar los contenedores de Kubernetes implementando los pods de vSphere o bien puede crear clústeres de Kubernetes ascendentes a través de VMware Tanzu™ Kubernetes Grid™ y ejecutar las aplicaciones dentro de estos clústeres.

Lea los siguientes temas a continuación:

- ¿Qué es vSphere IaaS control plane?
- ¿Qué es un espacio de nombres de vSphere?
- Flujos de trabajo y funciones de usuario de vSphere IaaS control plane
- ¿Cómo cambia vSphere IaaS control plane el entorno de vSphere?
- Licencias para vSphere IaaS control plane
- Gestión de identidad y acceso de vSphere IaaS control plane
- Seguridad de vSphere IaaS control plane

¿Qué es vSphere IaaS control plane?

Puede usar vSphere IaaS control plane para transformar vSphere en una plataforma para ejecutar cargas de trabajo de Kubernetes de forma nativa en la capa de hipervisor. Cuando se habilita en clústeres de vSphere, vSphere IaaS control plane proporciona la capacidad de ejecutar cargas de trabajo de Kubernetes directamente en hosts ESXi y de crear clústeres de Kubernetes ascendentes con espacios de nombres dedicados llamados espacio de nombres de vSphere.

Los desafíos de la pila de aplicaciones de hoy

Los sistemas distribuidos actuales se construyen con varios microservicios que normalmente ejecutan una gran cantidad de máquinas virtuales y pods de Kubernetes. Normalmente, una pila que no se basa en una vSphere IaaS control plane se compone de un entorno virtual subyacente, con una infraestructura de Kubernetes que se implementa dentro de las máquinas virtuales y los pods de Kubernetes correspondientes que también se ejecutan en estas máquinas virtuales. Tres funciones separadas controlan cada sector de la pila: los desarrolladores de aplicaciones, los administradores de clústeres de Kubernetes y los administradores de vSphere.

Figura 1-1. Pila de aplicaciones de hoy

Las diferentes funciones no tienen control ni visibilidad sobre los entornos de las demás:

- Como desarrollador de aplicaciones, puede ejecutar pods de Kubernetes, así como implementar y administrar aplicaciones basadas en Kubernetes. No tiene visibilidad sobre toda la pila que ejecuta cientos de aplicaciones.
- Como ingeniero de desarrollo y operaciones o administrador de clústeres, solo tiene control sobre la infraestructura de Kubernetes, sin las herramientas para administrar o supervisar el entorno virtual y resolver los problemas relacionados con recursos y otros problemas.
- Como administrador de vSphere, tiene control total sobre el entorno virtual subyacente, pero no tiene visibilidad sobre la infraestructura de Kubernetes, la colocación de los distintos objetos de Kubernetes en el entorno virtual y la forma en que estos consumen los recursos.

Las operaciones en la pila completa pueden ser desafiantes, ya que requieren comunicación entre las tres funciones. La falta de integración entre las diferentes capas de la pila también puede presentar desafíos. Por ejemplo, el programador de Kubernetes no tiene visibilidad sobre el inventario de vCenter Server y no puede colocar los pods de forma inteligente.

¿Cómo ayuda vSphere IaaS control plane?

vSphere IaaS control plane crea un plano de control de Kubernetes directamente en la capa de hipervisor. Como administrador de vSphere, puede activar los clústeres de vSphere existentes para vSphere IaaS control plane y así crear una capa de Kubernetes dentro de los hosts ESXi que forman parte de los clústeres. Los clústeres de vSphere activados para vSphere IaaS control plane se denominan Supervisores.

Figura 1-2. vSphere IaaS control plane

Al tener un plano de control de Kubernetes en la capa de hipervisor, se habilitan las siguientes capacidades en vSphere:

- Como administrador de vSphere, puede crear espacios de nombres en el Supervisor, denominados espacios de nombres de vSphere, y configurarlos con la cantidad especificada de memoria, CPU y almacenamiento. Puede proporcionar espacios de nombres de vSphere a los ingenieros de desarrollo y operaciones.
- Como ingeniero de desarrollo y operaciones, puede ejecutar cargas de trabajo de Kubernetes en la misma plataforma con grupos de recursos compartidos dentro de un espacio de nombres de vSphere. Puede implementar y administrar varios clústeres de Kubernetes ascendentes creados mediante Tanzu Kubernetes Grid. También puede implementar contenedores de Kubernetes directamente en el Supervisor dentro de un tipo especial de máquina virtual denominado pod de vSphere. También puede implementar máquinas virtuales comunes.
- Como administrador de vSphere, puede administrar y supervisar pods de vSphere, máquinas virtuales y clústeres de Tanzu Kubernetes Grid mediante el uso de vSphere Client.

- Como administrador de vSphere, tiene total visibilidad sobre los pods de vSphere y clústeres de Tanzu Kubernetes Grid que se ejecutan en diferentes espacios de nombres, su colocación en el entorno y la forma en que estos usan recursos.

La ejecución de Kubernetes en la capa de hipervisor también facilita la colaboración entre los administradores de vSphere y los equipos de ingenieros de desarrollo y operaciones, ya que ambas funciones trabajan con los mismos objetos.

¿Qué es una carga de trabajo?

En vSphere IaaS control plane, las cargas de trabajo son aplicaciones implementadas de una de las siguientes maneras:

- Aplicaciones que constan de contenedores que se ejecutan dentro de pods de vSphere.
- Cargas de trabajo aprovisionadas a través del servicio de máquina virtual.
- Clústeres de Tanzu Kubernetes Grid implementados mediante Tanzu Kubernetes Grid.
- Aplicaciones que se ejecutan dentro de los clústeres de Tanzu Kubernetes Grid.

¿Qué son las zonas de vSphere?

Las zonas de vSphere proporcionan alta disponibilidad frente a errores en el nivel de clúster en las cargas de trabajo implementadas en vSphere IaaS control plane. Como administrador de vSphere, puede crear zonas de vSphere en el vSphere Client y después asignar clústeres de vSphere a las zonas. Las zonas se utilizan para implementar Supervisores en el entorno de vSphere IaaS control plane.

Puede implementar un Supervisor en tres zonas de vSphere para alta disponibilidad en el nivel de clúster. También puede implementar un Supervisor en un solo clúster de vSphere, lo que creará una zona de vSphere automáticamente y se asignará al clúster, o bien puede utilizar un clúster que ya esté asignado a una zona. Para obtener más información, consulte Arquitectura de Supervisor y Implementaciones de clúster y de Supervisor zonal.

¿Qué es un clúster de Tanzu Kubernetes Grid?

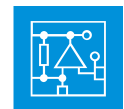
Un clúster de Tanzu Kubernetes Grid es una distribución completa de Kubernetes que VMware compila, firma y admite. Puede aprovisionar y operar clústeres de Tanzu Kubernetes Grid ascendentes en Supervisores mediante el uso de Tanzu Kubernetes Grid.

Un clúster de Tanzu Kubernetes Grid aprovisionado por Tanzu Kubernetes Grid tiene las siguientes características:

Un clúster de Tanzu Kubernetes Grid es:







Bien integrado



Preparado para producción



Totalmente compatible



Administrado por Kubernetes

- Instalación personalizada de Kubernetes. Tanzu Kubernetes Grid proporciona unos valores predeterminados adaptados y optimizados para que vSphere pueda aprovisionar clústeres de Tanzu Kubernetes Grid. El uso del Tanzu Kubernetes Grid puede ayudarle a reducir la cantidad de tiempo y esfuerzo que suele invertir en implementar y ejecutar un clúster de Kubernetes de nivel empresarial
- Integrado con la infraestructura de vSphere. Un clúster de Tanzu Kubernetes Grid se integra con la pila de SDDC de vSphere, lo que incluye el almacenamiento, las redes y la autenticación. Asimismo, un clúster de Tanzu Kubernetes Grid se basa en una instancia de Supervisor que se asigna clústeres de vSphere. Debido a esta estrecha integración, la ejecución de un clúster de Tanzu Kubernetes Grid resulta una experiencia de producto unificada.
- Listo para producción. Tanzu Kubernetes Grid aprovisiona clústeres de Tanzu Kubernetes Grid preparados para producción. Puede ejecutar cargas de trabajo de producción sin necesidad de realizar ninguna configuración adicional. Y, además, puede garantizar su disponibilidad y permitir que se realicen actualizaciones graduales del software de Kubernetes, así como ejecutar diferentes versiones de Kubernetes en clústeres distintos.
- Alta disponibilidad para cargas de trabajo de Kubernetes. Los clústeres de Tanzu Kubernetes Grid implementados en un Supervisor de vSphere de tres zonas están protegidos contra fallos en el nivel de clúster de vSphere. Los nodos de carga de trabajo y de plano de control de los clústeres de Tanzu Kubernetes Grid se distribuyen entre las tres zonas de vSphere, lo que hacen que las cargas de trabajo de Kubernetes se ejecutan en ellas tengan alta disponibilidad. Los clústeres de Tanzu Kubernetes Grid que se ejecutan en un Supervisor de una zona están protegidos contra fallos en el nivel de host ESXi, mediante vSphere HA.
- Totalmente compatible con VMware. Los clústeres de Tanzu Kubernetes Grid son de código abierto basado en Linux de VMware, se implementan en infraestructura de vSphere y se ejecutan en hosts ESXi. Si tiene problemas con cualquiera de las capas de la pila (desde el hipervisor hasta el clúster de Kubernetes), VMware es el único proveedor con el que necesita ponerse en contacto.

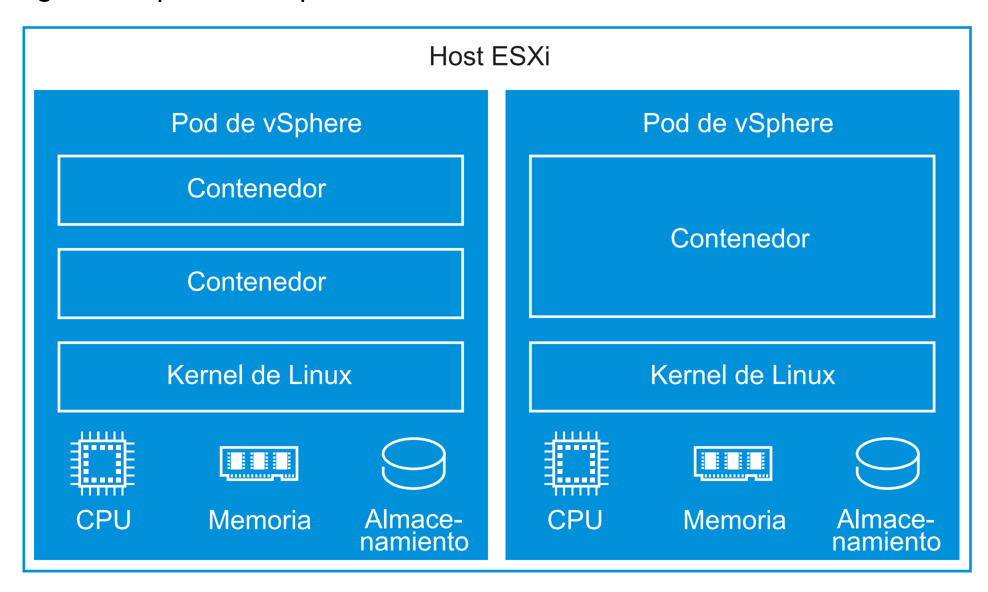
- Administrado por Kubernetes. Los clústeres de Tanzu Kubernetes Grid se compilan a partir del Supervisor, que también es un clúster de Kubernetes. Un clúster de Tanzu Kubernetes Grid se define en el espacio de nombres de vSphere mediante un recurso personalizado. Los clústeres de Tanzu Kubernetes Grid se aprovisionan de forma independiente mediante comandos kubectl conocidos y la CLI de Tanzu. Todo el sistema de herramientas mantiene una coherencia: tanto si aprovisiona un clúster como si distribuye cargas de trabajo, utilizará los mismos comandos, el lenguaje YAML habitual y los flujos de trabajo comunes.

Para obtener más información, consulte Capítulo 3 Arquitectura y componentes del Tanzu Kubernetes Grid y *Uso del servicio TKG con el plano de control de IaaS de vSphere*.

¿Qué es un pod de vSphere?

vSphere IaaS control plane introduce una construcción llamada pod de vSphere, que equivale a un pod de Kubernetes. Una pod de vSphere es una máquina virtual con un tamaño pequeño que ejecuta uno o más contenedores de Linux. Cada pod de vSphere tiene un tamaño preciso para la carga de trabajo que aloja y tiene reservas de recursos explícitas para esa carga de trabajo. Asigna la cantidad exacta de recursos de almacenamiento, memoria y CPU necesarios para la ejecución de la carga de trabajo. Los pods de vSphere solo se admiten con Supervisores que estén configurados con NSX como pila de redes.

Figura 1-3. pods de vSphere



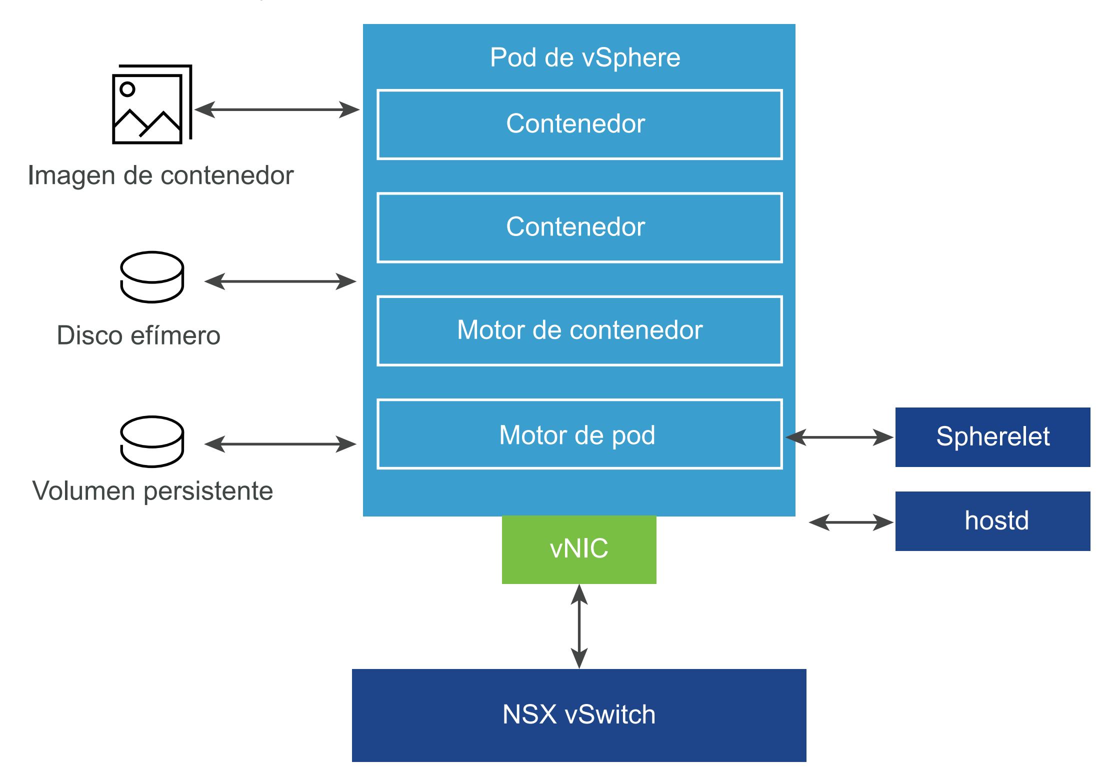
Los pods de vSphere son objetos en vCenter Server y habilitan las siguientes capacidades para las cargas de trabajo:

- Aislamiento fuerte. Un pod de vSphere está aislado del mismo modo que una máquina virtual. Cada pod de vSphere tiene su propio kernel único de Linux basado en el kernel utilizado en Photon OS. En lugar de muchos contenedores que comparten un kernel, como en una configuración nativa, en un pod de vSphere, cada contenedor tiene un kernel de Linux único

- Gestión de recursos. vSphere DRS controla la colocación de los pods de vSphere en el Supervisor.
- Alto rendimiento. Los pods de vSphere obtienen el mismo nivel de aislamiento de recursos que las máquinas virtuales, lo que elimina los problemas de vecinos ruidosos a la vez que mantiene el tiempo de inicio rápido y una baja sobrecarga de los contenedores.
- Diagnóstico. Como administrador de vSphere, puede utilizar todas las herramientas de introspección y supervisión que están disponibles con vSphere en las cargas de trabajo.

Los pods de vSphere son compatibles con Open Container Initiative (OCI) y pueden ejecutar contenedores desde cualquier sistema operativo, siempre y cuando estos contenedores también sean compatibles con OCI.

Figura 1-4. Redes y almacenamiento de instancias de pod de vSphere



Los pods de vSphere utilizan tres tipos de almacenamiento en función de los objetos que se almacenen; respectivamente, VMDK efímeros, VMDK de volumen persistente y VMDK de imagen de contenedor. Como administrador de vSphere, debe configurar directivas de almacenamiento para la colocación de la memoria caché de imagen de contenedor y VMDK efímeros en el nivel de Supervisor. En un nivel de espacio de nombres de vSphere, debe configurar las directivas de almacenamiento para la colocación de volúmenes persistentes. Consulte Almacenamiento persistente para cargas de trabajo para obtener más información sobre los requisitos y conceptos de almacenamiento con vSphere IaaS control plane.

Para las redes, las instancias de pods de vSphere y las máquinas virtuales de los clústeres de Tanzu Kubernetes Grid utilizan la topología proporcionada por NSX. Para obtener más información, consulte Redes del Supervisor.

Spherelet es un proceso adicional que se crea en cada host. Se trata de un kubelet que se transporta de forma nativa a ESXi y permite que el host ESXi se convierta en parte del clúster de Kubernetes.

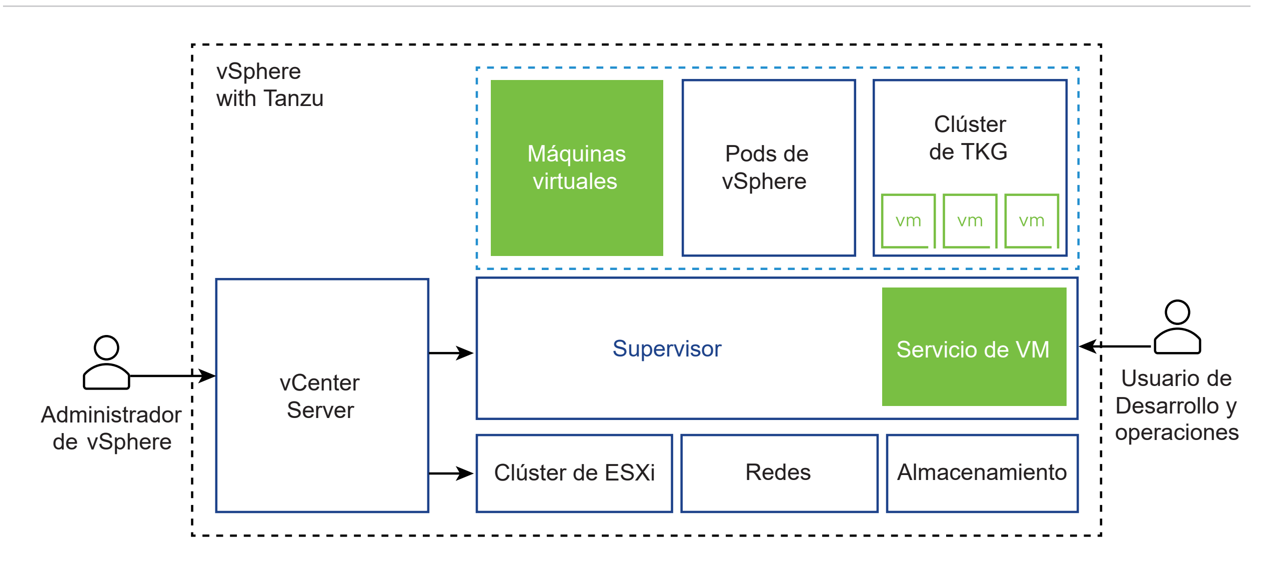
Para obtener información sobre el uso de pods de vSphere en Supervisores consulte Implementar cargas de trabajo en pods de vSphere en la documentación de *Servicios y cargas de trabajo del plano de control de IaaS de vSphere*.

Usar máquinas virtuales en vSphere IaaS control plane

vSphere IaaS control plane ofrece una funcionalidad de servicio de máquina virtual que permite a los ingenieros de desarrollo y operaciones implementar y ejecutar máquinas virtuales, además de contenedores, en un entorno de Kubernetes común y compartido. Tanto contenedores como máquinas virtuales comparten los mismos recursos de espacio de nombres de vSphere y se pueden administrar a través de una única interfaz de vSphere IaaS control plane.

El servicio de máquina virtual responde a las necesidades de los equipos de desarrollo y operaciones que usan Kubernetes, pero tienen cargas de trabajo basadas en máquinas virtuales existentes que no se pueden colocar en contenedores fácilmente. También ayuda a los usuarios a reducir la sobrecarga de administrar una plataforma que no es de Kubernetes junto con una plataforma de contenedor. Al ejecutar contenedores y máquinas virtuales en una plataforma de Kubernetes, los equipos de desarrollo y operaciones pueden consolidar su marca de carga de trabajo en una sola plataforma.

Nota Además de las máquinas virtuales independientes, el servicio de máquina virtual administra las máquinas virtuales que conforman los clústeres de Tanzu Kubernetes Grid. Para obtener información acerca de los clústeres, consulte la documentación de *Uso del servicio TKG con el plano de control de IaaS de vSphere*.



Cada máquina virtual implementada a través del servicio de máquina virtual funciona como una máquina completa que ejecuta todos los componentes, incluido su propio sistema operativo, sobre la infraestructura de vSphere IaaS control plane. La máquina virtual tiene acceso a las redes y al almacenamiento que proporciona Supervisor, y se administra mediante el comando estándar `kubectl` de Kubernetes. La máquina virtual se ejecuta como un sistema completamente aislado que está a prueba de interferencias de otras máquinas virtuales o cargas de trabajo en el entorno de Kubernetes.

¿Cuándo utilizar máquinas virtuales en una plataforma de Kubernetes?

Por lo general, la decisión de ejecutar cargas de trabajo en un contenedor o en una máquina virtual depende de sus necesidades y objetivos empresariales. Entre los motivos para utilizar las máquinas virtuales aparecen los siguientes:

- Las aplicaciones no se pueden poner en contenedores.
- Las aplicaciones están diseñadas para un kernel personalizado o un sistema operativo personalizado.
- Las aplicaciones son más adecuadas para ejecutarse en una máquina virtual.
- Desea tener una experiencia de Kubernetes coherente y evitar la sobrecarga. En lugar de ejecutar conjuntos separados de infraestructura para las plataformas de contenedor y que no son de Kubernetes, puede consolidar estas pilas y administrarlas con un comando de `kubectl` familiar.

Para obtener información sobre la implementación y la administración de máquinas virtuales independientes en un Supervisor, consulte Implementar y administrar máquinas virtuales en la documentación de *Servicios y cargas de trabajo del plano de control de IaaS de vSphere*.

servicios de supervisor en vSphere IaaS control plane

servicios de supervisor son operadores de Kubernetes certificados por vSphere que ofrecen a los desarrolladores componentes de infraestructura como servicio y servicios de proveedores de software independientes perfectamente integrados. Puede instalar y administrar servicios de supervisor en el entorno de vSphere IaaS control plane para que estén disponibles para su uso con cargas de trabajo de Kubernetes. Cuando se instalan servicios de supervisor en Supervisores, los ingenieros de desarrollo y operaciones pueden utilizar las API de servicio para crear Supervisores en sus espacios de nombres de usuario. A continuación, estas instancias se pueden consumir en pods de vSphere y clústeres de Tanzu Kubernetes Grid.

Obtenga más información sobre los servicios de supervisor compatibles y cómo descargar sus archivos YAML de servicio en http://vmware.com/go/supervisor-service.

Para obtener información sobre cómo utilizar servicios de supervisor, consulte Administrar servicios de Supervisor en la documentación de *Servicios y cargas de trabajo del plano de control de IaaS de vSphere*.

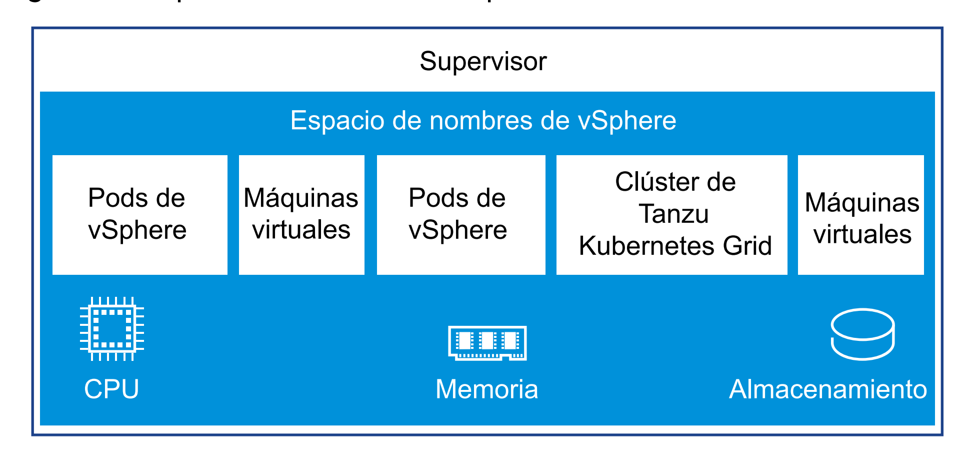
¿Qué es un espacio de nombres de vSphere?

Un espacio de nombres de vSphere establece los límites de recursos en los que se pueden ejecutar pods de vSphere, máquinas virtuales y clústeres de Tanzu Kubernetes Grid. Como administrador de vSphere, puede crear y configurar espacios de nombres de vSphere a través de vSphere Client.

Cuando se crea inicialmente, el espacio de nombres de vSphere tiene recursos ilimitados dentro del Supervisor. Como administrador de vSphere, puede establecer límites para la CPU, la memoria y el almacenamiento, así como la cantidad de objetos de Kubernetes que se pueden ejecutar en el espacio de nombres de vSphere. Las limitaciones de almacenamiento se representan como cuotas de almacenamiento en Kubernetes. Se crea un grupo de recursos en vSphere por cada espacio de nombres de vSphere en el Supervisor.

En un Supervisor activado en las Zonas de vSphere, se crea un grupo de recursos de espacio de nombres en cada clúster de vSphere que se asigna a una zona. El espacio de nombres de vSphere se distribuye entre los tres clústeres de vSphere que forman parte de las Zonas de vSphere. Los recursos utilizados para un espacio de nombres de vSphere en un Supervisor de tres zonas se toman de los tres clústeres de vSphere subyacentes a partes iguales. Por ejemplo, si dedica 300 MHz de CPU, se toman 100 MHz de cada clúster de vSphere.

Figura 1-5. espacio de nombres de vSphere



Para otorgar acceso a los espacios de nombres al ingeniero de desarrollo y operaciones, como administrador de vSphere, debe asignar permisos a los usuarios o a los grupos de usuarios disponibles en un origen de identidad que esté asociado con vCenter Single Sign-On o que provenga de un proveedor de OIDC que esté registrado en el Supervisor. Para obtener más información, consulte Gestión de identidad y acceso de vSphere IaaS control plane.

Después de crear un espacio de nombres y configurarlo con límites de recursos y objetos, así como con permisos y directivas de almacenamiento, como ingeniero de desarrollo y operaciones, puede acceder al espacio de nombres para ejecutar cargas de trabajo como clústeres de Tanzu Kubernetes Grid, pods de vSphere y máquinas virtuales creadas a través del servicio de máquina virtual.

Diferencias entre un espacio de nombres de vSphere y un espacio de nombres de Kubernetes

Aunque en su núcleo un espacio de nombres de vSphere cumple la misma función que un espacio de nombres de Kubernetes, un espacio de nombres de vSphere es específico de vSphere IaaS control plane. No debe confundir un espacio de nombres de vSphere con un espacio de nombres de Kubernetes.

Un espacio de nombres de vSphere se implementa como una extensión de un grupo de recursos de vSphere y su función es proporcionar recursos a las cargas de trabajo que se ejecutan en el Supervisor. Un espacio de nombres de vSphere tiene una asignación directa a un espacio de nombres de Kubernetes a través de la cual se aplican cuotas de almacenamiento y objetos en las cargas de trabajo.

Otra diferencia con un espacio de nombres de Kubernetes normal es que el administrador de vSphere administra el acceso de los usuarios a los espacios de nombres de vSphere, como se mencionó anteriormente. El administrador de vSphere también puede asociar clases de máquinas virtuales y bibliotecas de contenido que contienen plantillas de máquina virtual que pueden usar los ingenieros de desarrollo y operaciones para realizar el autoservicio de las máquinas virtuales. Para obtener información, consulte Implementar y administrar máquinas virtuales en *Servicios y cargas de trabajo del plano de control de IaaS de vSphere*.

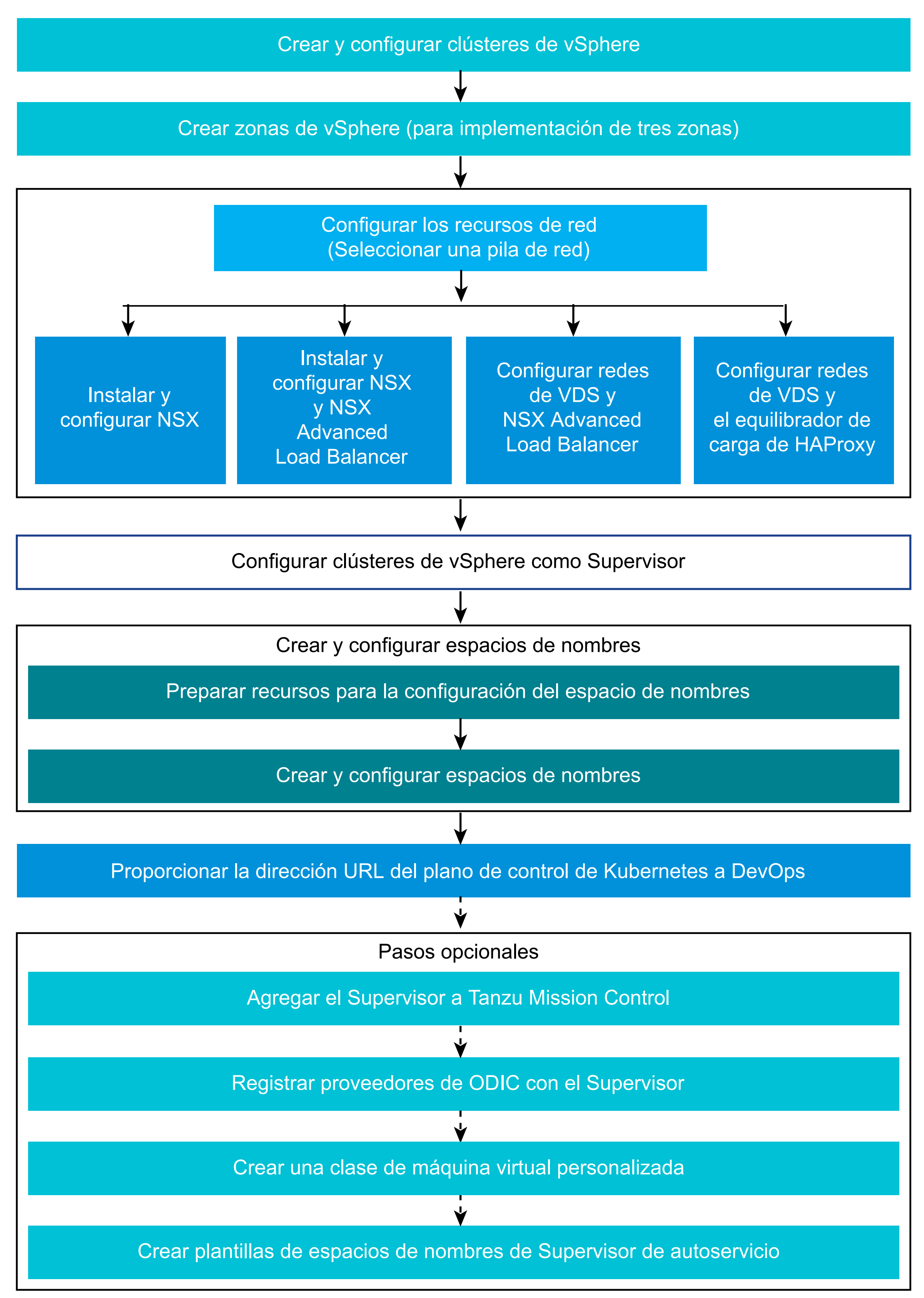
Flujos de trabajo y funciones de usuario de vSphere IaaS control plane

vSphere IaaS control plane involucra dos funciones: el administrador de vSphere y el ingeniero de desarrollo y operaciones. El ingeniero de desarrollo y operaciones consta de la función de desarrollo y operaciones, desarrollador de aplicaciones y administrador de Kubernetes. Ambas funciones interactúan con la plataforma a través de diferentes interfaces y pueden tener usuarios o grupos de usuarios definidos para ellas en vCenter Server con permisos asociados. Los flujos de trabajo de las funciones de administrador de vSphere y de ingeniero de desarrollo y operaciones son distintos y se determinan según el área específica de conocimientos que estas requieren.

Flujos de trabajo y funciones de usuario

Como administrador de vSphere, la interfaz principal a través de la cual interactúa con vSphere IaaS control plane es vSphere Client. En un nivel alto, sus responsabilidades implican la configuración de una instancia de Supervisor y espacios de nombres, donde los ingenieros de desarrollo y operaciones pueden implementar cargas de trabajo de Kubernetes. Debe tener un excelente conocimiento sobre vSphere, NSX Advanced Load Balancer o el equilibrador de carga de HAProxy, NSX (si selecciona esta pila de redes) y conocimientos básicos sobre Kubernetes.

Figura 1-6. Flujo de trabajo de alto nivel de administrador de vSphere



Como ingeniero de desarrollo y operaciones, puede ser desarrollador de Kubernetes y propietario de aplicaciones, administrador de Kubernetes o una combinación de ambas funciones. Como ingeniero de desarrollo y operaciones, puede utilizar comandos kubectl para implementar pods de vSphere y máquinas virtuales en un espacio de nombres existente, y puede usar kubectl y CLI de Tanzu para implementar y administrar clústeres de Tanzu Kubernetes Grid. Por lo general, como ingeniero de desarrollo y operaciones, no tiene que ser un experto en vSphere, NSX, vDS o NSX Advanced Load Balancer y HAProxy, sino que basta con que tenga conocimientos básicos sobre estas tecnologías y la plataforma para interactuar con los administradores de vSphere de forma más eficiente.

Figura 1-7. Flujo de trabajo de alto nivel de ingeniero de desarrollo y operaciones

Obtener información necesaria del administrador de vSphere

Iniciar sesión en el Supervisor y obtener contextos

Implementar cargas de trabajo de Kubernetes

Seleccionar un método

1.

2.

Implementar clústeres de Tanzu Kubernetes Grid

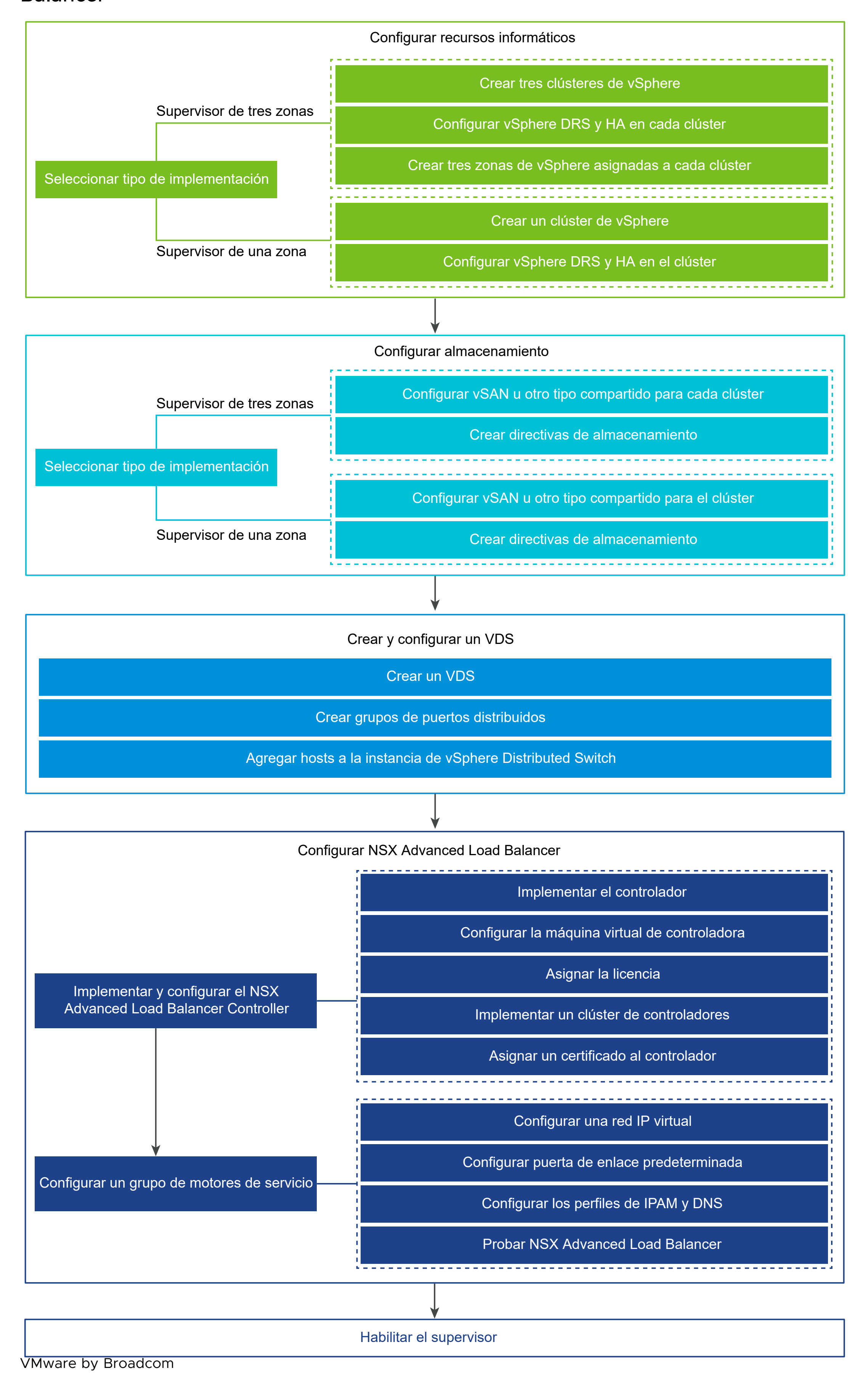
Implementar pods de vSpherey máquinas virtuales

Realizar operaciones de CRUD a través de clústeres de Tanzu Kubernetes Grid, pods de vSphere y máquinas virtuales

Supervisor con redes VDS y flujo de trabajo de NSX Advanced Load Balancer

Como administrador de vSphere, puede configurar clústeres de vSphere como un Supervisor con la pila de redes de vSphere a través de un VDS y NSX Advanced Load Balancer. Puede configurar un Supervisor de una zona asignado a un clúster de vSphere o un Supervisor de tres zonas asignado a tres clústeres de vSphere. Para obtener más información sobre los requisitos del sistema, consulte Requisitos para la implementación de clústeres de Supervisor con redes VDS y NSX Advanced Load Balancer y Requisitos para la implementación de Supervisor zonal con redes VDS y NSX Advanced Load Balancer. Para obtener información sobre cómo habilitar un Supervisor con redes VDS, consulte Instalar y configurar en *Instalar y configurar el plano de control de IaaS de vSphere*.

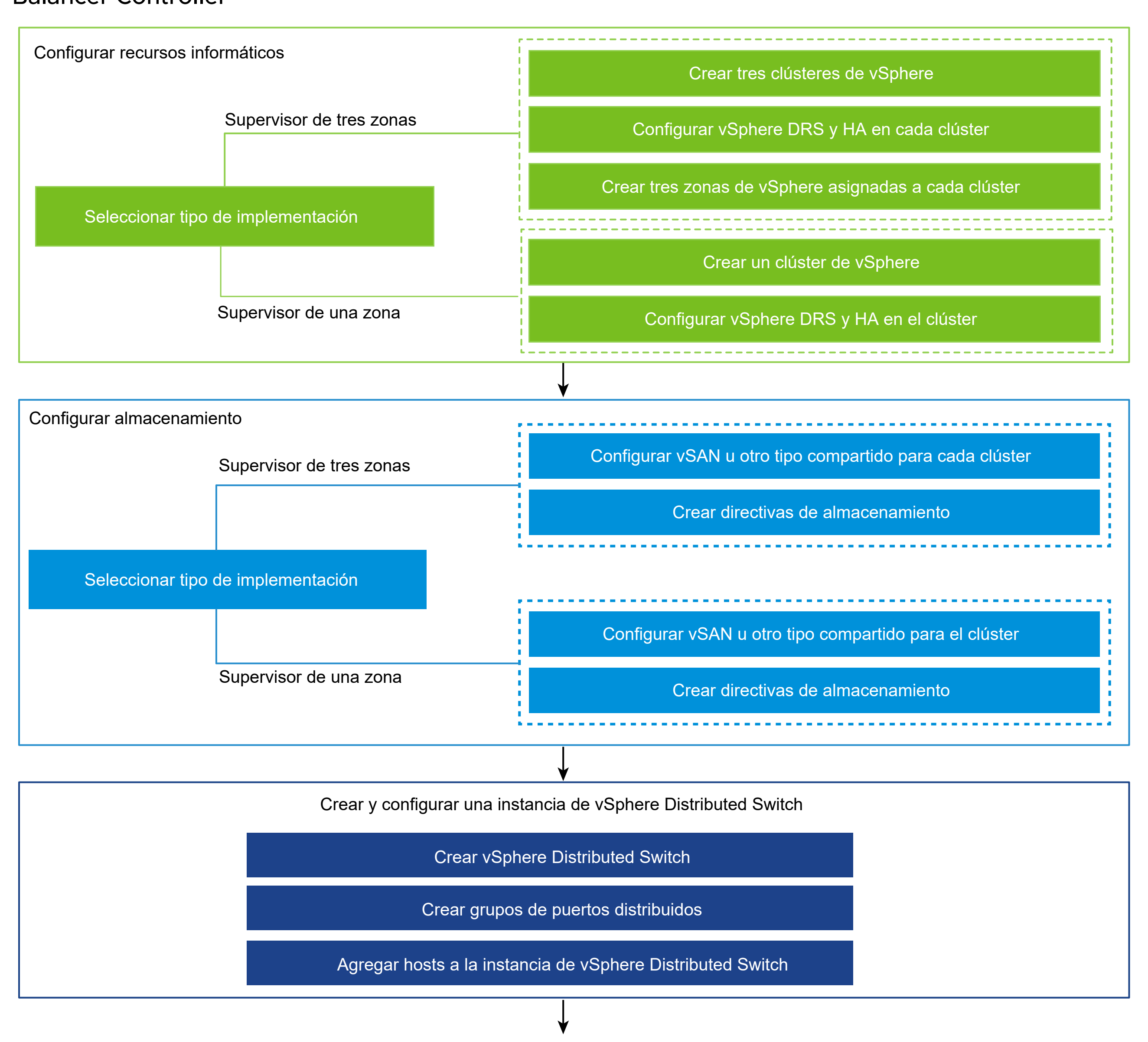
Figura 1-8. Flujo de trabajo para habilitar un Supervisor con redes VDS y NSX Advanced Load Balancer

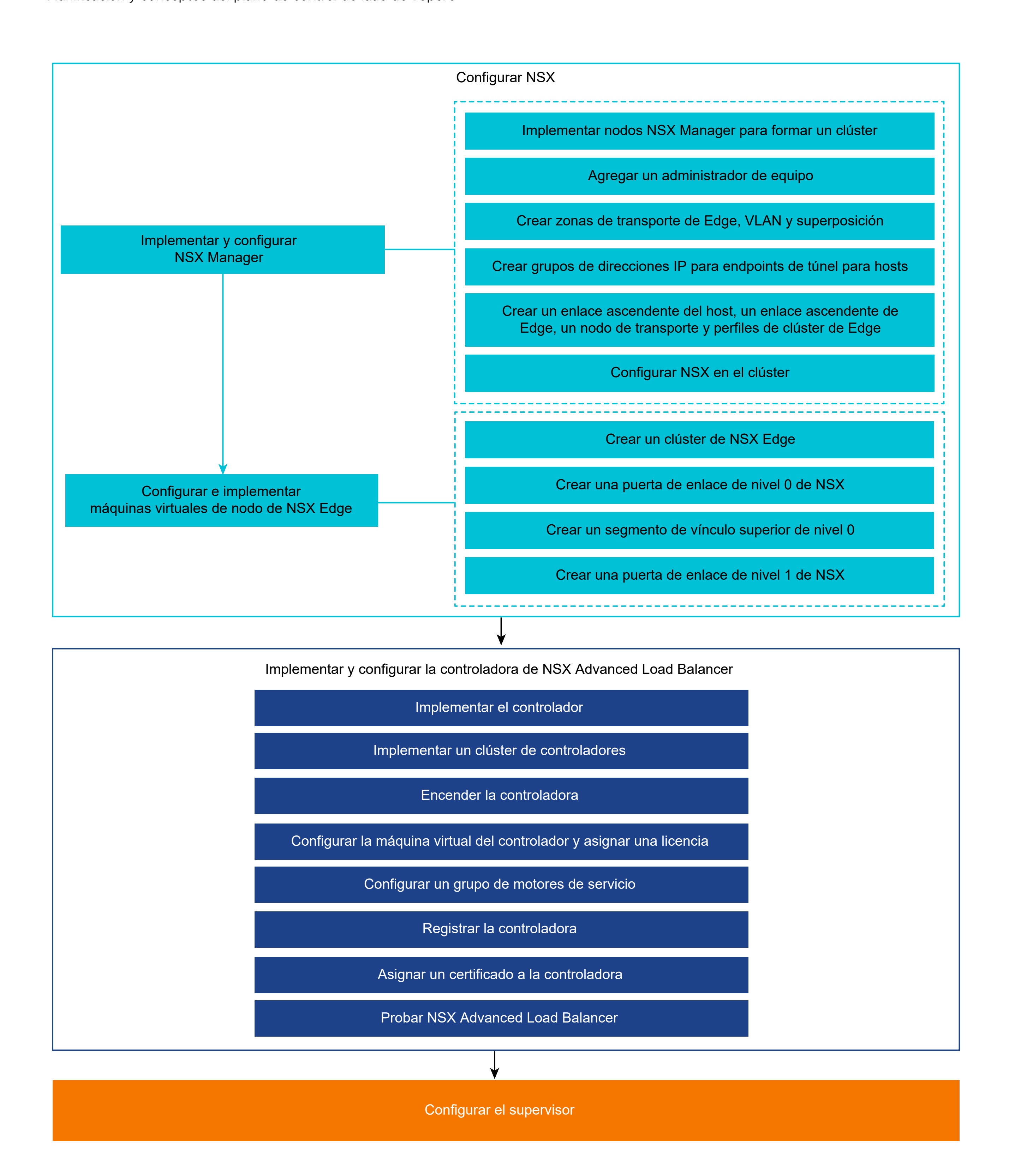


Supervisor con redes de NSX y flujo de trabajo de la NSX Advanced Load Balancer Controller

Puede configurar un Supervisor de una zona o de tres zonas con la pila de redes NSX y la NSX Advanced Load Balancer Controller. Para obtener más información sobre los requisitos, consulte Requisitos para la implementación de Supervisor del clúster con NSX y NSX Advanced Load Balancer y Requisitos para Supervisor zonal con NSX y NSX Advanced Load Balancer. Para ver el procedimiento de instalación, consulte Instalar y configurar NSX y NSX Advanced Load Balancer.

Figura 1-9. Flujo de trabajo para habilitar un supervisor con redes NSX y la NSX Advanced Load Balancer Controller

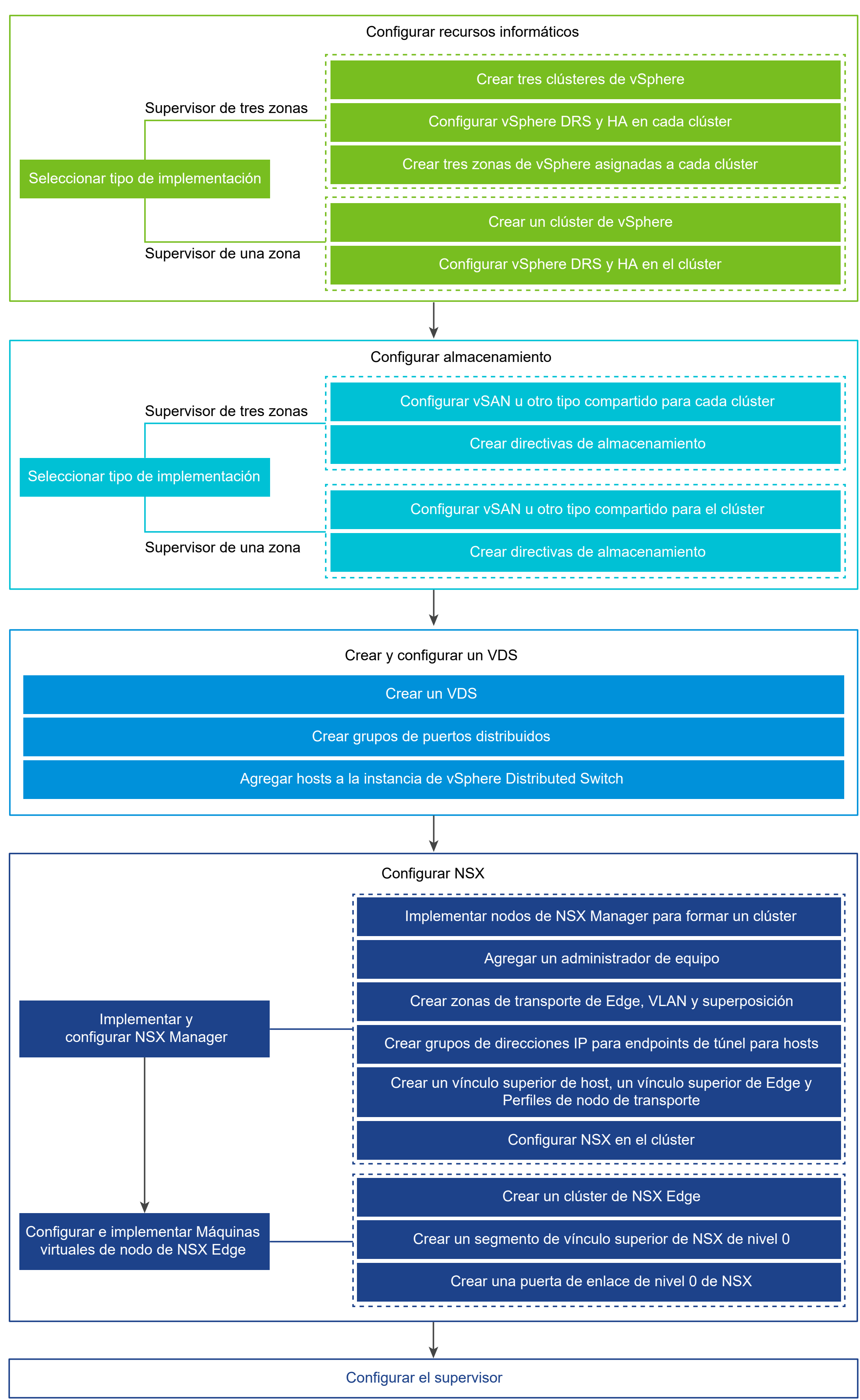



Configurar NSX
Implementar y configurar NSX Manager
Implementar nodos NSX Manager para formar un clúster
Agregar un administrador de equipo
Crear zonas de transporte de Edge, VLAN y superposición
Crear grupos de direcciones IP para endpoints de túnel para hosts
Crear un enlace ascendente del host, un enlace ascendente de Edge, un nodo de transporte y perfiles de clúster de Edge
Configurar NSX en el clúster
Configurar e implementar máquinas virtuales de nodo de NSX Edge
Crear un clúster de NSX Edge
Crear una puerta de enlace de nivel 0 de NSX
Crear un segmento de vínculo superior de nivel 0
Crear una puerta de enlace de nivel 1 de NSX
Implementar y configurar la controladora de NSX Advanced Load Balancer
Implementar el controlador
Implementar un clúster de controladores
Encender la controladora
Configurar la máquina virtual del controlador y asignar una licencia
Configurar un grupo de motores de servicio
Registrar la controladora
Asignar un certificado a la controladora
Probar NSX Advanced Load Balancer
Configurar el supervisor

Supervisor con flujo de trabajo de redes NSX

También puede configurar un Supervisor de una o tres zonas con NSX como pila de redes.
Para obtener más información sobre los requisitos del sistema, consulte Requisitos para la implementación de clústeres de Supervisor con NSX y Requisitos para Supervisor zonal con NSX.
Para obtener instrucciones de instalación, consulte Instalar y configurar en *Instalar y configurar el plano de control de IaaS de vSphere*.

Figura 1-10. Flujo de trabajo para habilitar un supervisor con redes NSX



Supervisor con redes VDS y flujo de trabajo del equilibrador de carga de HAProxy

Como administrador de vSphere, puede habilitar un Supervisor en una o tres zonas de vSphere asignadas a clústeres de vSphere mediante la pila de redes VDS y el equilibrador de carga de HAProxy. Para obtener más información sobre los requisitos del sistema, consulte Requisitos para la implementación de clústeres de Supervisor con redes VDS y equilibrador de carga de HAProxy y Requisitos para la implementación de un Supervisor zonal con equilibrador de carga de HAProxy. Para obtener instrucciones de instalación, consulte Instalar y configurar en *Instalar y configurar el plano de control de IaaS de vSphere*.

Figura 1-11. Flujo de trabajo para habilitar un supervisor con redes VDS y HAProxy

Configurar recursos informáticos
Supervisor de tres zonas
Crear tres clústeres de vSphere
Configurar vSphere DRS y HA en cada clúster
Crear tres zonas de vSphere asignadas a cada clúster
Seleccionar tipo de implementación
Supervisor de una zona
Crear un clúster de vSphere
Configurar vSphere DRS y HA en el clúster

Configurar almacenamiento
Supervisor de tres zonas
Configurar vSAN u otro tipo compartido para cada clúster
Crear directivas de almacenamiento
Seleccionar tipo de implementación
Supervisor de una zona
Configurar vSAN u otro tipo compartido para el clúster
Crear directivas de almacenamiento

Crear y configurar un VDS
Crear un VDS
Crear grupos de puertos distribuidos para la red de cargas de trabajo
Agregar hosts a la instancia de vSphere Distributed Switch

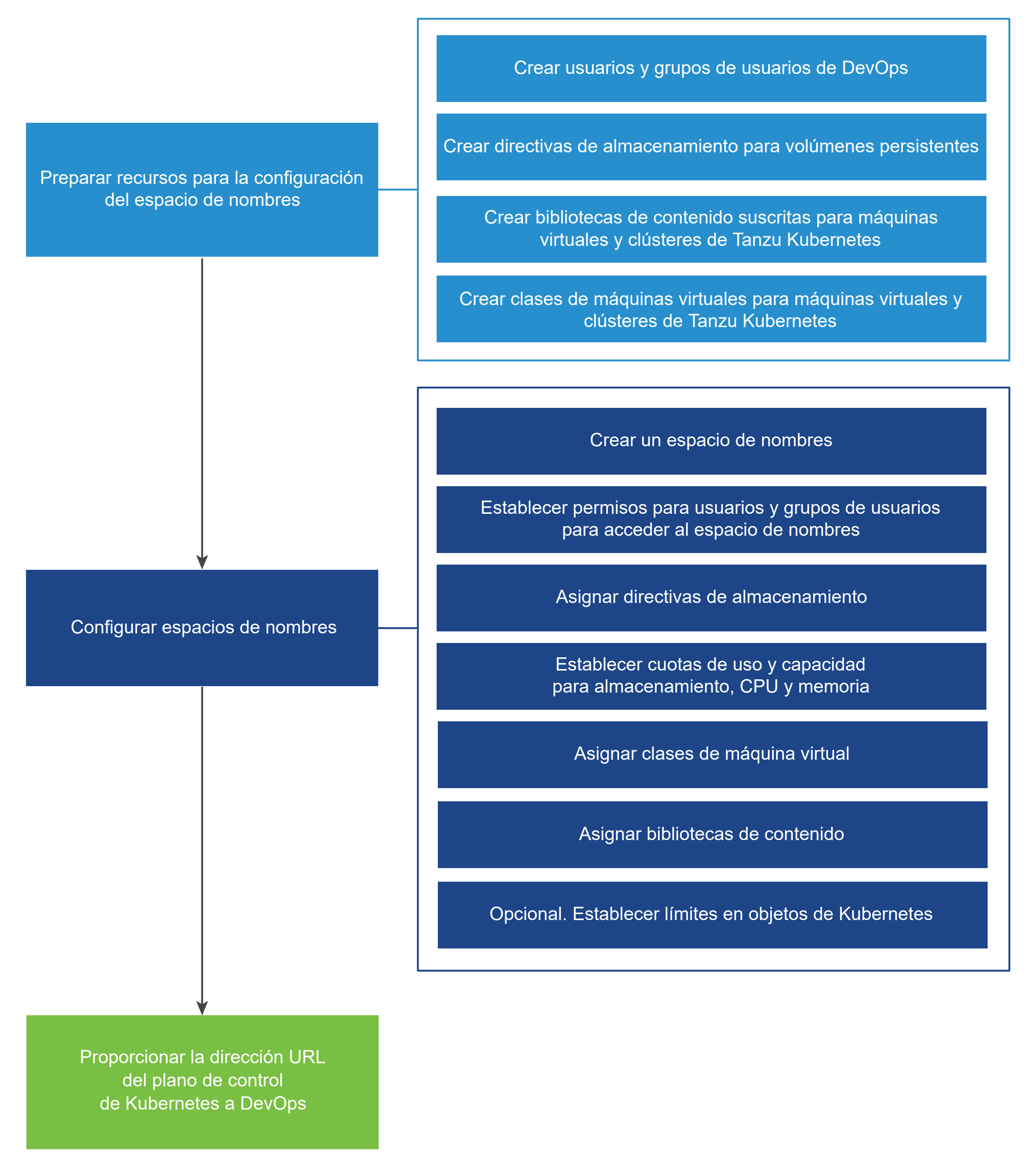
Instalar y configurar el equilibrador de carga de HAProxy

Habilitar el supervisor

Flujo de trabajo de creación y configuración de espacios de nombres

Una vez que habilite un Supervisor, como administrador de vSphere cree y configure espacios de nombres de vSphere en el Supervisor. Debe recopilar los requisitos de recursos específicos de los ingenieros de Desarrollo y operaciones para las aplicaciones y cargas de trabajo que desean ejecutar, y configurar los espacios de nombres según corresponda. Para obtener más información consulte Configurar y administrar espacios de nombres de vSphere.

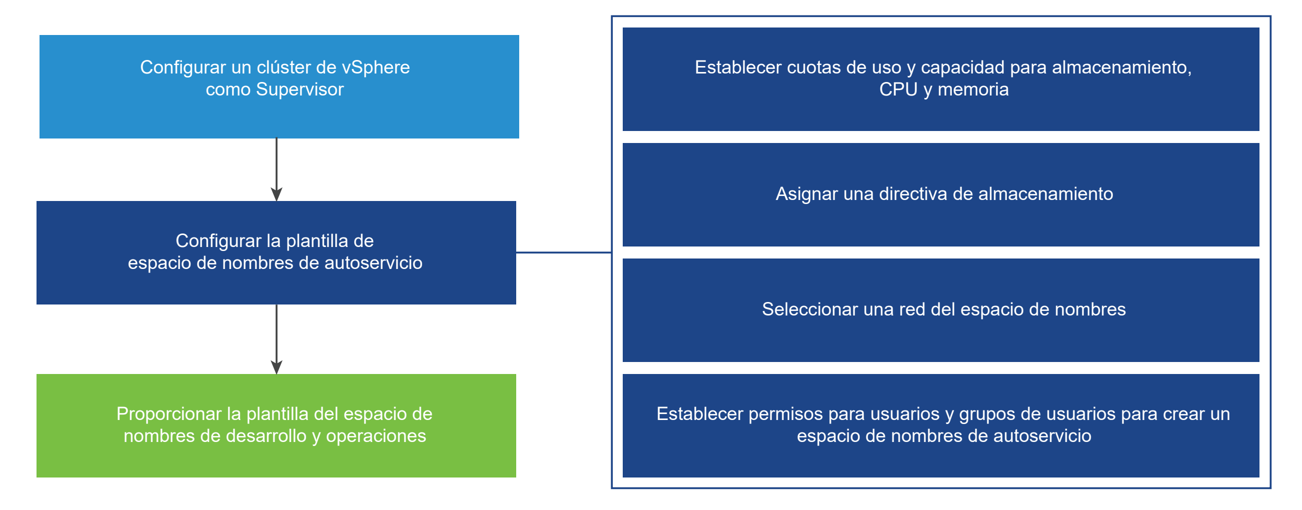
Figura 1-12. Flujo de trabajo para configurar espacios de nombres de vSphere



Flujo de trabajo de creación y configuración de espacios de nombres de autoservicio

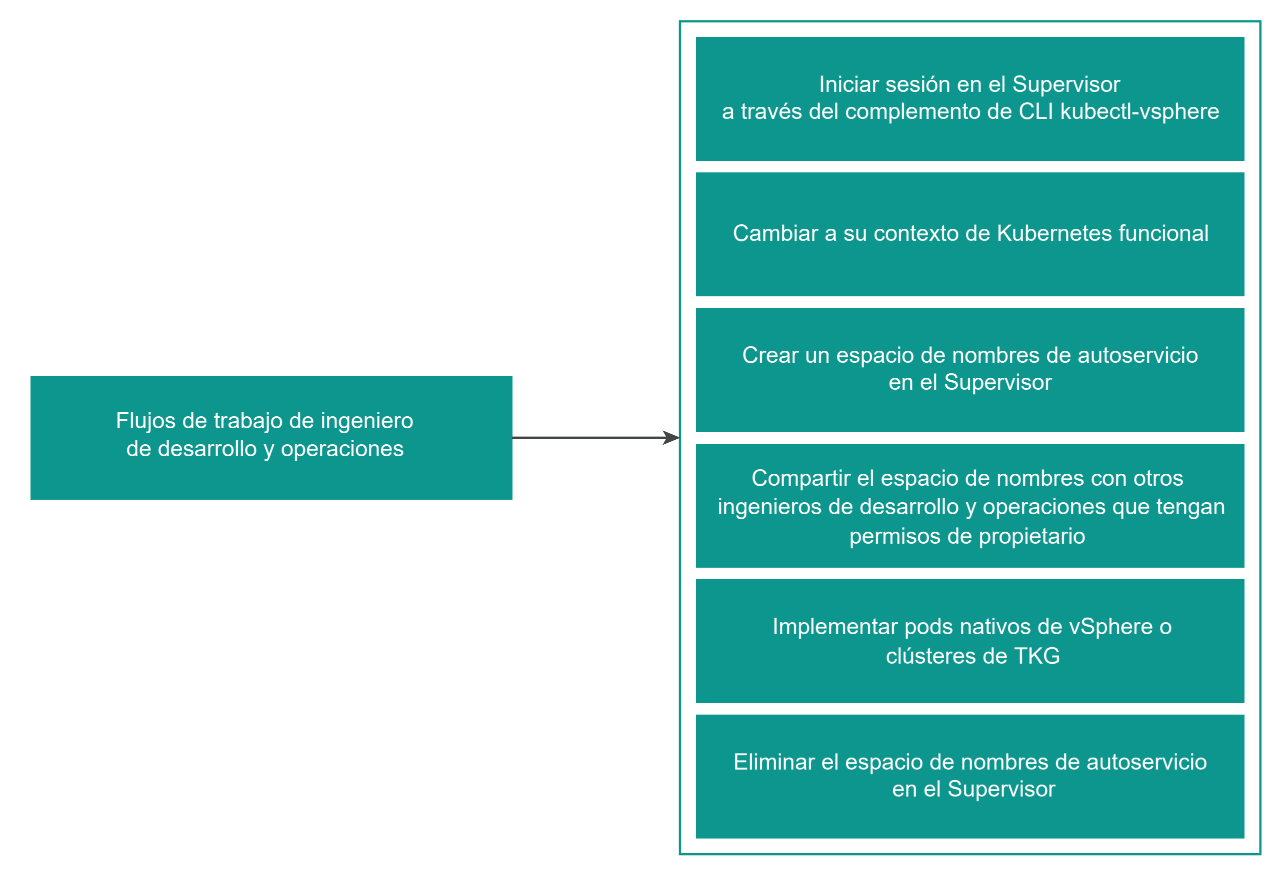
Como administrador de vSphere, puede crear un espacio de nombres de vSphere, establecer límites de CPU, memoria y almacenamiento en el espacio de nombres, asignar permisos y aprovisionar o activar el servicio de espacio de nombres en un clúster como plantilla. Para obtener más información consulte Configurar y administrar espacios de nombres de vSphere.

Figura 1-13. Flujo de trabajo de aprovisionamiento de plantilla de espacio de nombres de autoservicio



Como ingeniero de Desarrollo y operaciones, puede crear un espacio de nombres de vSphere mediante autoservicio e implementar cargas de trabajo dentro de él. Puede compartirlo con otros ingenieros de Desarrollo y operaciones, o eliminarlo cuando ya no sea necesario.

Figura 1-14. Flujo de trabajo de creación de espacio de nombres de autoservicio



Flujo de trabajo de aprovisionamiento de máquinas virtuales y pod de vSphere

Como ingeniero de Desarrollo y operaciones, puede implementar pods de vSphere y máquinas virtuales dentro de los límites de recursos de un espacio de nombres que se ejecuta en un Supervisor. Para obtener más información, consulte Implementar cargas de trabajo en pods de vSphere e Implementar y administrar máquinas virtuales en *Servicios y cargas de trabajo del plano de control de IaaS de vSphere*.

Figura 1-15. Flujo de trabajo de aprovisionamiento de máquinas virtuales y pods de vSphere

Flujo de trabajo de aprovisionamiento del clúster de Tanzu Kubernetes Grid

Como ingeniero de Desarrollo y operaciones, puede crear y configurar clústeres de Tanzu Kubernetes Grid en espacios de nombres de vSphere. Para obtener más información, consulte la guía *Uso del servicio TKG con el plano de control de IaaS de vSphere*.

¿Cómo cambia vSphere IaaS control plane el entorno de vSphere?

Un Supervisor agrega objetos al inventario de vCenter Server, como espacios de nombres, pods de vSphere y clústeres de Tanzu Kubernetes Grid.

En cada Supervisor, puede ver:

- Espacios de nombres que representan aplicaciones lógicas que se ejecutan en el clúster.
- Grupos de recursos de cada espacio de nombres en Supervisor. En una implementación de tres zonas se crea un grupo de recursos para cada espacio de nombres en cada parte del clúster de una zona.

En cada espacio de nombres, puede ver:

- pods de vSphere.
- Clústeres de Tanzu Kubernetes Grid.
- Máquinas virtuales independientes y máquinas virtuales del plano de control de Kubernetes.
- Recursos de redes y almacenamiento.
- Permisos de usuario para ese espacio de nombres.

Licencias para vSphere IaaS control plane

Conozca cuáles son las diferentes licencias que puede asignar al Supervisor y cómo funcionan el cumplimiento de licencias, el período de evaluación y la caducidad de las licencias.

Licencias de una instancia de Supervisor

Después de activar un Supervisor en clústeres de vSphere, puede utilizar el conjunto completo de funcionalidades del Supervisor dentro de un período de evaluación de 60 días. Debe asignar una licencia válida al Supervisor antes de que venza el período de evaluación de 60 días.

Licencias de soluciones VCF y VVF

A partir de la versión vSphere 8 Update 2b, puede utilizar las licencias de la solución VMware vSphere Foundation (VVF) o VMware Cloud Foundation (VCF) para vSphere IaaS control plane. Una vez que actualice vCenter Server a la versión 8 Update 2b, puede asignar la licencia de la solución VVF o VCF a los Supervisores en el entorno de vSphere.

Nota Las claves de licencia de componentes individuales siguen siendo compatibles. Se proporcionan junto con la licencia de la solución. En su entorno, puede utilizar la licencia de la solución, las licencias de componentes individuales o una combinación de ambas.

Licencias de Tanzu Edition

Si ejecuta vSphere 8 Update 2b y su Supervisor ya tiene una licencia válida de Tanzu Edition, la licencia seguirá funcionando hasta que caduque. Una vez que caduque la licencia de Tanzu, debe asignar la licencia de la solución VCF o VVF al Supervisor o una licencia de Tanzu válida.

Caducidad de licencias

Cuando caduca una licencia de la solución o una licencia de Tanzu Edition, puede seguir usando el conjunto completo de capacidades de vSphere IaaS control plane hasta que adquiera licencias nuevas. Sin embargo, no puede asignar la licencia caducada en nuevos Supervisores.

Caducidad del período de evaluación

Cuando caduca el período de evaluación de un Supervisor, como administrador de vSphere no puede crear nuevos espacios de nombres de vSphere ni actualizar la versión de Kubernetes del Supervisor. Como ingeniero de desarrollo y operaciones, no puede implementar nuevas cargas de trabajo ni realizar cambios en la configuración de los clústeres de Tanzu Kubernetes Grid existentes, como agregar nodos nuevos.

Puede seguir implementando cargas de trabajo en clústeres de Tanzu Kubernetes Grid, y todas las cargas de trabajo existentes seguirán funcionando según lo esperado. Todas las cargas de trabajo de Kubernetes que ya se han implementado continúan con su funcionamiento normal.

Conformidad de licencias

Una licencia de la solución o una clave de licencia de Tanzu tiene una capacidad por CPU de hasta 32 núcleos por CPU, de forma similar a las licencias de host ESXi. Cuando se asigna una de estas licencias a un Supervisor, la cantidad de capacidad consumida se determina en función del número de CPU en los hosts de los clústeres y la cantidad de núcleos en cada CPU. Puede asignar una licencia de la solución o una clave de licencia de Tanzu Edition a varios Supervisores a la vez, pero no puede asignar varias claves de licencia a un Supervisor.

Si amplía un Supervisor agregando nuevos hosts, por ejemplo, y la clave de licencia que asignó al Supervisor se queda sin capacidad, puede seguir usando la misma clave de licencia. Sin embargo, para seguir cumpliendo con el CLUF, debe adquirir una nueva clave de licencia con capacidad suficiente para cubrir todas las CPU y núcleos del Supervisor

Licencias para vSphere IaaS control plane

Según la pila de redes con la que haya configurado vSphere IaaS control plane, las licencias proporcionadas varían:

Configuración de Supervisor	Licencias para vSphere 8 Update 2b	Licencias antes de vSphere 8 Update 2b
Supervisor con NSX Advanced Load Balancer y redes de VDS	■ Licencia de la solución VCF ■ Licencia de vSphere Enterprise+ ■ Licencia de Tanzu Edition ■ NSX Advanced Load Balancer Essentials	■ Licencia de vSphere Enterprise+ ■ Licencia de Tanzu Edition ■ NSX Advanced Load Balancer Essentials
Supervisor con redes de VDS y equilibrador de carga de HAProxy	■ Licencia de la solución VVF ■ Licencia de vSphere Enterprise+ ■ Licencia de Tanzu Edition	■ Licencia de vSphere Enterprise+ ■ Licencia de Tanzu Edition
Supervisor con NSX	■ Licencia de la solución VVF ■ Licencia de vSphere Enterprise+ ■ Licencia de Tanzu Edition ■ NSX Advanced o superior	■ Licencia de vSphere Enterprise+ ■ Licencia de Tanzu Edition ■ NSX Advanced o superior
Supervisor con NSX y NSX Advanced Load Balancer	■ Licencia de la solución VCF ■ NSX Advanced Load Balancer Enterprise ■ Licencia de vSphere Enterprise+ ■ Licencia de Tanzu Edition ■ NSX Advanced o superior ■ NSX Advanced Load Balancer Enterprise	■ Licencia de vSphere Enterprise+ ■ Licencia de Tanzu Edition ■ NSX Advanced o superior ■ NSX Advanced Load Balancer Enterprise

Gestión de identidad y acceso de vSphere IaaS control plane

Como administrador de vSphere, necesita privilegios para activar y configurar un Supervisor y para administrar los espacios de nombres de vSphere. Defina los permisos en los espacios de nombres para determinar qué ingenieros y desarrolladores de Desarrollo y operaciones pueden acceder a ellos. También puede configurar el Supervisor con un proveedor externo de OpenID Connect (OIDC) para habilitar la autenticación multifactor. Como ingeniero o desarrollador de Desarrollo y operaciones, se autentica con Supervisor mediante las credenciales de vCenter Single Sign-On o las credenciales de un proveedor de OIDC, en función de lo que el administrador de vSphere haya configurado para usted en el Supervisor. Solo puede acceder a los espacios de nombres de vSphere para los que tiene permisos.

Proveedores de identidades compatibles

vSphere IaaS control plane admite los siguientes proveedores de identidad:

- vCenter Single Sign-On. El proveedor de identidad predeterminado que utiliza para autenticarse con el entorno de vSphere IaaS control plane, incluidos los Supervisores y los clústeres de Tanzu Kubernetes Grid. vCenter Single Sign-On proporciona autenticación para la infraestructura de vSphere y se puede integrar con sistemas AD/LDAP. Para obtener más información sobre vCenter Single Sign-On, consulte Autenticación de vSphere con vCenter Single Sign-On.

- Proveedor de identidad externo. Como administrador de vSphere, puede configurar un Supervisor con un proveedor de identidad externo que admita el protocolo OpenID Connect. Una vez configurado con un proveedor de identidad externo, el Supervisor funciona como un cliente de OAuth 2.0 y utiliza el servicio de autenticación Pinniped para conectarse a los clústeres de Tanzu Kubernetes Grid mediante la CLI de Tanzu. La CLI de Tanzu admite el aprovisionamiento y la administración del ciclo de vida de los clústeres de Tanzu Kubernetes Grid. Cada instancia de Supervisor puede admitir un proveedor de identidad externo.

Autenticación con el Supervisor

Las diferentes funciones que interactúan con vSphere IaaS control plane pueden utilizar los siguientes métodos para autenticarse con Supervisor:

- Administrador de vSphere. Como administrador de vSphere, utilice vCenter Single Sign-On para autenticarse con vSphere a través de vSphere Client. También puede utilizar el complemento de vSphere para kubectl para autenticarse con los clústeres de Supervisor y Tanzu Kubernetes Grid a través de kubectl. Para obtener más información, consulte Conectar a Supervisor como usuario de vCenter Single Sign-On.
- Ingeniero o desarrollador de desarrollo y operaciones. Como desarrollador o ingeniero de desarrollo y operaciones, utiliza vCenter Single Sign-On para autenticarse con Supervisor a través del complemento de vSphere para kubectl y kubectl. También puede conectarse a un Supervisor mediante credenciales de un proveedor de identidad externo que esté configurado con ese Supervisor. Para obtener más información, consulte Conectarse a clústeres de TKG en Supervisor mediante un proveedor de identidad externo.

Iniciar sesiones con Supervisor

Cuando haya iniciado sesión en Supervisor como usuario de vCenter Single Sign-On, un proxy de autenticación redirigirá la solicitud a vCenter Single Sign-On. El complemento de vSphere para kubectl establece una sesión con vCenter Server y obtiene un token de autenticación de vCenter Single Sign-On. También obtiene una lista de los espacios de nombres de vSphere a los que tiene acceso y rellena la configuración con estos espacios de nombres de vSphere. La lista de espacios de nombres de vSphere se actualiza en el siguiente inicio de sesión si hay cambios en los permisos de su cuenta de usuario.

La cuenta que utiliza para iniciar sesión en el Supervisor proporciona acceso solo a los espacios de nombres de vSphere que se le asignan. Para iniciar sesión en vCenter Server, el administrador de vSphere debe establecer los permisos adecuados en su cuenta en uno o en varios espacios de nombres de vSphere.

Nota La sesión de kubectl dura 10 horas. Después de que caduque la sesión, debe volver a autenticarse con Supervisor. Al cerrar sesión, el token se elimina del archivo de configuración de su cuenta de usuario, pero sigue siendo válido hasta que finalice la sesión.

Autenticarse con clústeres de Tanzu Kubernetes Grid

Como ingeniero o desarrollador de desarrollo y operaciones, se conecta a clústeres de Tanzu Kubernetes Grid aprovisionados para operar en ellos y administrarlos. Cuando se concede el permiso de edición o propietario a una cuenta de usuario en el espacio de nombres de vSphere en el que se aprovisiona el clúster de Tanzu Kubernetes Grid, a la cuenta se le asigna la función `cluster-admin`. Como alternativa, también puede utilizar el usuario `kubernetes-admin` para conectarse a Tanzu Kubernetes Grid. También puede conceder a los desarrolladores acceso a los clústeres de Tanzu Kubernetes Grid enlazando un usuario o grupo a la directiva de seguridad de pods predeterminada o personalizada. Para obtener más información, consulte Conectarse a clústeres de TKG en Supervisor mediante la autenticación de vCenter SSO y Conectarse a clústeres de TKG en Supervisor mediante un proveedor de identidad externo.

Permisos de función de los espacios de nombres de vSphere

Como administrador de vSphere, puede conceder permisos de vista, edición o propietario a los ingenieros o desarrolladores de desarrollo y operaciones. en los espacios de nombres de vSphere. Sus usuarios o grupos deben estar disponibles en vCenter Single Sign-On o en un proveedor de identidad externo configurado con Supervisor. Un usuario o un grupo puede tener acceso a varios espacios de nombres de vSphere. Cada función de espacio de nombres de vSphere permite las siguientes acciones:

Función	Descripción
Puede ver	Acceso de solo lectura para el usuario o el grupo. El usuario o el grupo pueden iniciar sesión en el plano de control del Supervisor y crear una lista con las cargas de trabajo que se ejecutan en el espacio de nombres de vSphere, como los pods de vSphere y los clústeres de Tanzu Kubernetes Grid, y las máquinas virtuales.
Puede editar	El usuario o el grupo pueden crear, leer, actualizar y eliminar pods de vSphere, clústeres de Tanzu Kubernetes Grid y máquinas virtuales. Los usuarios que forman parte del grupo Administradores tienen permisos de edición en todos los espacios de nombres del Supervisor.
Propietario	Los usuarios o los grupos con permisos de propietario pueden: ■ Implementar y administrar cargas de trabajo en el espacio de nombres de vSphere. ■ Compartir el espacio de nombres de vSphere con otros usuarios o grupos. ■ Crear y eliminar espacios de nombres de vSphere adicionales mediante kubectl. Cuando usuarios con el permiso de propietario comparten el espacio de nombres, pueden asignar permisos de vista, edición o propietario a otros usuarios o grupos. **Nota** La función de propietario es compatible con los usuarios disponibles en vCenter Single Sign-On. No se puede usar la función de propietario con un usuario o grupo que provenga de un proveedor de identidad externo.

Para obtener información sobre cómo crear una configuración de los espacios de nombres de vSphere, consulte Crear y configurar un espacio de nombres de vSphere.

Como administrador de vSphere, tras configurar un espacio de nombres de vSphere con permisos de función, cuotas de recursos y almacenamiento, debe proporcionar la URL del plano de control de Supervisor a los ingenieros y desarrolladores de desarrollo y operaciones, quienes la utilizan para iniciar sesión en el plano de control. Una vez iniciada la sesión, los ingenieros y desarrolladores de desarrollo y operaciones pueden acceder a los espacios de nombres de vSphere para los que tienen permisos en todos los Supervisores configurados con los mismos proveedores de identidad que pertenecen a un sistema vCenter Server. Cuando los sistemas vCenter Server se encuentran en Enhanced Linked Mode, los ingenieros y desarrolladores de desarrollo y operaciones pueden acceder a todos los espacios de nombres de vSphere para los que tienen permisos en todos los Supervisores disponibles en el grupo de Linked Mode. La dirección IP del plano de control de Supervisor es una dirección IP virtual generada por NSX o un equilibrador de carga en el caso de las redes de VDS para que actúe como punto de acceso al plano de control de Supervisor.

Permisos de administrador de vSphere

Como administrador de vSphere, por lo general, su cuenta de usuario puede tener los siguientes permisos:

Objeto	Permisos
usuario de vCenter Single Sign-On	Grupo Administradores
usuario de espacios de nombres de vSphere	A los miembros del grupo Administradores se les conceden permisos de edición en todos los espacios de nombres de vSphere.

En función de la interfaz que utilice para interactuar con vSphere IaaS control plane, puede realizar diferentes operaciones con los permisos que le hayan concedido:

Interfaz	Operaciones
vSphere Client	Cuando inicie sesión como administrador en vSphere Client, puede: ■ Activar y configurar Supervisores. ■ Crear y configurar espacios de nombres de vSphere con asignaciones de recursos y permisos de función para desarrolladores o ingenieros de desarrollo y operaciones. Se requieren permisos de función en los espacios de nombres de vSphere para los usuarios o los grupos que deseen iniciar sesión en el plano de control de Supervisor a través de kubectl para ejecutar y administrar cargas de trabajo. ■ Implementar y administrar el servicio de supervisor en Supervisores.
kubectl	Si inició sesión en el plano de control de Supervisor con una cuenta de administrador de vCenter Single Sign-On, puede: ■ Ver recursos en todos los espacios de nombres de vSphere, incluidos los espacios de nombres de vSphere del sistema (kube-system y todos los espacios de nombres vmware-system-*) ■ Editar los recursos de todos los espacios de nombres de vSphere que no son del sistema, que son espacios de nombres creados a través de las API de vSphere Client o vCenter Server. Sin embargo, cuando se inicia sesión en el plano de control de Supervisor con una cuenta que forma parte del grupo Administradores, no se permite editar ningún recurso en el nivel del clúster, crear espacios de nombres de vSphere mediante kubectl ni crear enlaces de funciones. Debe utilizar vSphere Client como la interfaz principal para establecer cuotas de recursos, crear y configurar espacios de nombres de vSphere, y configurar permisos de usuario.

Permisos de ingenieros y desarrolladores de desarrollo y operaciones

Como ingeniero o desarrollador de desarrollo y operaciones, por lo general, su cuenta de usuario necesita los siguientes permisos:

Objeto	Permisos
espacios de nombres de vSphere	Editar o propietario
usuario de vCenter Single Sign-On	Ninguno o Solo lectura

Como ingeniero o desarrollador de desarrollo y operaciones, puede utilizar kubectl como interfaz principal para interactuar con vSphere IaaS control plane. Debe poder iniciar sesión en el plano de control de Supervisor a través del complemento de vSphere para kubectl para ver, ejecutar y administrar cargas de trabajo en los espacios de nombres de vSphere que tiene asignados. Por lo tanto, su cuenta de usuario necesita permisos de edición o propietario en uno o varios espacios de nombres de vSphere.

Normalmente, no es necesario realizar ninguna operación administrativa en los Supervisores a través de vSphere Client. Sin embargo, en algunos casos, es posible que desee iniciar sesión en vSphere Client para ver los recursos y las cargas de trabajo en los espacios de nombres de vSphere que están asignados a su cuenta. Con este fin, es posible que necesite permisos de solo lectura en vSphere.

Privilegios de espacios de nombres de vSphere

Los privilegios de espacios de nombres de vSphere controlan cómo interactúa con vSphere IaaS control plane. Puede establecer un privilegio en los diferentes niveles de la jerarquía. Por ejemplo, si se establece un privilegio en el nivel de carpeta, se puede propagar el privilegio a uno o más objetos dentro de la carpeta. El objeto que aparece en la columna Obligatorio en debe tener establecido el privilegio, de manera directa o heredada.

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Permite operaciones de retiro de disco	Permite realizar operaciones de retirada de almacenes de datos.	Almacenes de datos	Namespaces.ManageDisks
Archivos de componentes de cargas de trabajo de copia de seguridad	Permite realizar una copia de seguridad del contenido del clúster etcd (solo se utiliza en VMware Cloud on AWS).	Clústeres	Namespaces.Backup
Espacios de nombres accesibles en lista	Permite enumerar los espacios de nombres de vSphere accesibles.	Clústeres	Namespaces.ListAccess
Modificar configuración de todo el clúster	Permite modificar la configuración de Supervisor, así como crear y eliminar los espacios de nombres de vSphere.	Clústeres	Namespaces.ManageCapabilities

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Modificar configuración de autoservicio del espacio de nombres en todo el clúster	Permite modificar la configuración de autoservicio del espacio de nombres de vSphere.	Clústeres (para activar y desactivar) Plantillas (para modificar la configuración) vCenter Server (para crear una plantilla)	Namespaces.SelfServiceManage
Modificar configuración del espacio de nombres	Permite modificar las opciones de configuración del espacio de nombres de vSphere, como la asignación de recursos, los permisos de usuario y las asociaciones de bibliotecas de contenido.	Clústeres	Namespaces.Manage
Alternar capacidades de clúster	Permite manipular el estado de las capacidades del clúster Supervisor (se utiliza internamente solo para VMware Cloud on AWS).	Clústeres	No corresponde
Actualizar clústeres a versiones más recientes	Permite el inicio de la actualización de Supervisor.	Clústeres	Namespaces.Upgrade

Privilegios de servicios de supervisor

Los privilegios de los servicios de supervisor controlan quién puede crear y administrar servicios de supervisor en el entorno de vSphere IaaS control plane.

Tabla 1-1. Privilegios de servicios de supervisor

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Administrar servicios de supervisor	Permite crear, actualizar o eliminar un servicio de supervisor. También permite instalar un servicio de supervisor en un Supervisor y crear o eliminar una versión del servicio de supervisor.	Clústeres	SupervisorServices.Manage

Privilegios de clases de máquinas virtuales

Los privilegios de clases de máquinas virtuales controlan quién puede agregar y eliminar clases de máquinas virtuales en un espacio de nombres de vSphere.

Tabla 1-2. Privilegios de clases de máquinas virtuales

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Administrar clases de máquinas virtuales	Permite administrar clases de máquinas virtuales en los espacios de nombres de vSphere en un Supervisor.	Clústeres	VirtualMachineClasses.Manage

Privilegios de vistas de almacenamiento

Con los privilegios de vistas de almacenamiento, podrá ver las directivas de almacenamiento en vCenter Server para poder asignarlas a los espacios de nombres de vSphere.

Tabla 1-3. Privilegios de vistas de almacenamiento

Nombre del privilegio en vSphere Client	Descripción	Necesario para	Nombre de privilegio en la API
Configurar servicio	Permite a los usuarios con privilegios utilizar todas las API del servicio de supervisión de almacenamiento. Utilice **Vistas de almacenamiento.Ver** para los privilegios sobre las API de solo lectura del servicio de supervisión de almacenamiento.	vCenter Server raíz	StorageViews.ConfigureService
Ver	Permite a los usuarios con privilegios utilizar las API de solo lectura del servicio de supervisión de almacenamiento.	vCenter Server raíz	StorageViews.View

Seguridad de vSphere IaaS control plane

vSphere IaaS control plane aprovecha las funciones de seguridad de vSphere y aprovisiona los clústeres de Tanzu Kubernetes Grid que sean seguros de forma predeterminada.

vSphere IaaS control plane es un módulo complementario para vSphere que puede aprovechar las funciones de seguridad integradas en vCenter Server y ESXi. Para obtener más información, consulte la documentación de Seguridad de vSphere.

Supervisor cifra todos los secretos almacenados en la base de datos (etcd). Los secretos se cifran a través de un archivo de clave de cifrado local, que vCenter Server proporciona en el arranque. La clave de descifrado se almacena en la memoria (tempfs) en los nodos de Supervisor y en el disco de forma cifrada dentro de la base de datos de vCenter Server. La clave está disponible en texto no cifrado para los usuarios raíz de cada sistema. Los secretos que se encuentran en la base de datos de cada clúster de carga de trabajo se almacenan en texto no cifrado. Todas las conexiones etcd se autentican con certificados que se generan en la instalación y se rotan durante las actualizaciones. Actualmente no es posible rotar o actualizar manualmente los certificados. El mismo modelo de cifrado se aplica a los datos de la base de datos (etcd) que está instalada en el plano de control de cada clúster de Tanzu Kubernetes Grid.

En un Supervisor puede ejecutar pods de vSphere confidenciales en sistemas compatibles. Puede crear pods de vSphere confidenciales agregando el estado de cifrado SEV (Secure Encrypted Virtualization-Encrypted State, SEV-ES) como una mejora de seguridad. Para obtener más información, consulte Implementar un pod de vSphere confidencial en *Servicios y cargas de trabajo del plano de control de IaaS de vSphere*.

Un clúster de Tanzu Kubernetes Grid está protegido de forma predeterminada. La instancia restrictiva de PodSecurityPolicy (PSP) está disponible para cualquier clúster de Tanzu Kubernetes Grid. Si los desarrolladores necesitan ejecutar contenedores raíz o pods con privilegios, al menos un administrador de clústeres deberá crear un objeto RoleBinding que otorgue acceso de usuario a la PSP con privilegios predeterminada. Para obtener más información, consulte *Uso del servicio TKG con el plano de control de IaaS de vSphere*.

Un clúster de Tanzu Kubernetes Grid no tiene credenciales de infraestructura. Las credenciales que se almacenan en un clúster de Tanzu Kubernetes Grid solo son suficientes para acceder al espacio de nombres de vSphere donde el clúster de Tanzu Kubernetes Grid es tenant. Por ello, no existe la posibilidad de realizar la escalación de privilegios para los operadores de clústeres ni los usuarios.

El token de autenticación utilizado para acceder a un clúster de Tanzu Kubernetes Grid tiene un ámbito tal que el token no se puede usar para acceder al Supervisor o a otros clústeres de Tanzu Kubernetes Grid. De este modo, se evita que los operadores del clúster, o los individuos que puedan intentar poner en peligro un clúster, utilicen el acceso de nivel raíz para capturar un token de administrador de vSphere cuando inicien sesión en un clúster de Tanzu Kubernetes Grid.

Arquitectura y componentes del Supervisor

2

Los clústeres activados con vSphere IaaS control plane se denominan Supervisores. Puede seleccionar entre una implementación de tres zonas, en la cual se habilita un Supervisor en tres clústeres de vSphere, o bien puede seleccionar una asignación uno a uno entre un clúster de vSphere y un Supervisor. Los Supervisores son la base de vSphere IaaS control plane que proporciona los componentes y los recursos necesarios para ejecutar cargas de trabajo que incluyen pods de vSphere, máquinas virtuales y clústeres de Tanzu Kubernetes Grid.

Lea los siguientes temas a continuación:

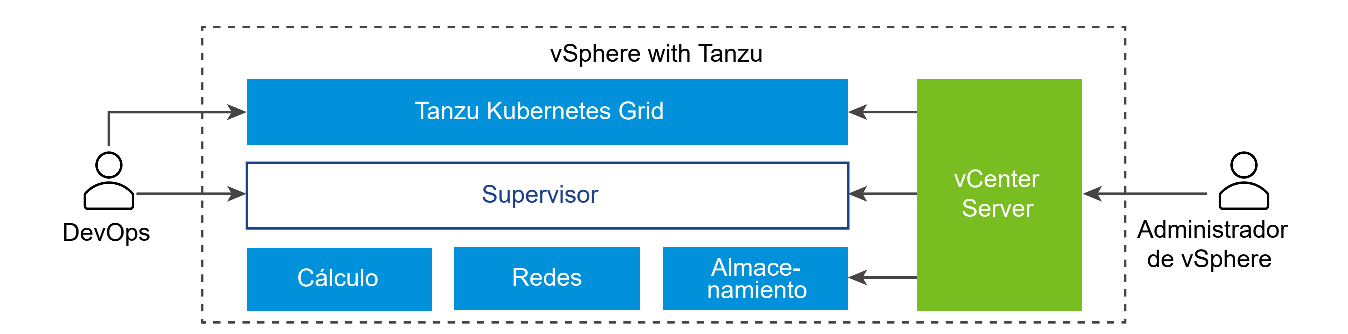
- Arquitectura de Supervisor
- Redes del Supervisor
- Almacenamiento de Supervisor

Arquitectura de Supervisor

Cuando se habilita vSphere IaaS control plane en clústeres de vSphere y se convierten en Supervisores, el plano de control de Kubernetes se crea dentro de la capa del hipervisor. Esta capa contiene objetos específicos que habilitan la capacidad para ejecutar cargas de trabajo de Kubernetes en ESXi.

Figura 2-1. Arquitectura general de Supervisor

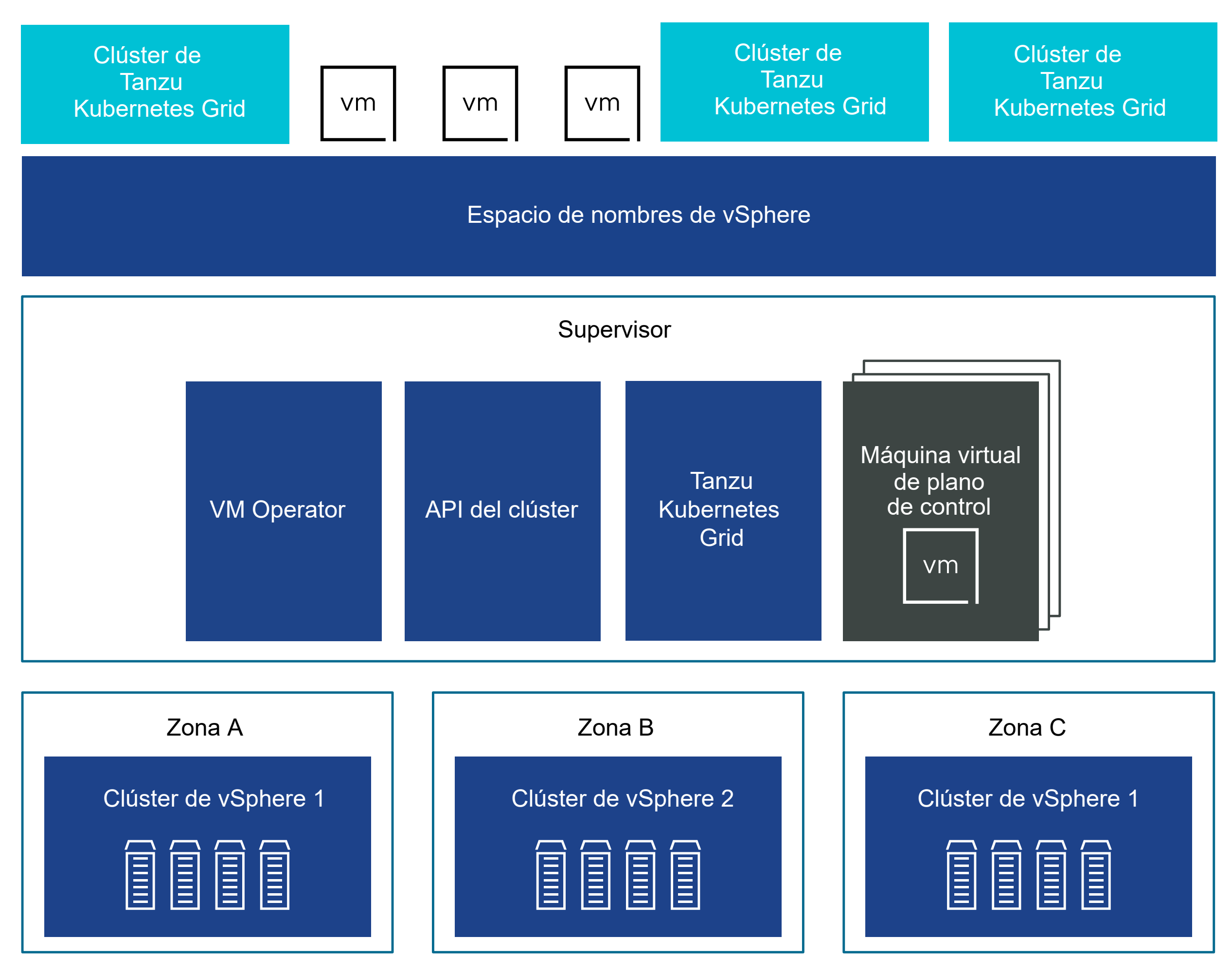
El diagrama muestra la arquitectura de alto nivel de vSphere IaaS control plane, con Tanzu Kubernetes Grid en la parte superior, el Supervisor en el centro y, a continuación, ESXi, las redes y el almacenamiento en la parte inferior, donde vCenter Server se encarga de administrarlos.



Un Supervisor se ejecuta sobre una capa de SDDC compuesta por ESXi para recursos informáticos, NSX o redes VDS y vSAN u otra solución de almacenamiento compartido. El almacenamiento compartido se utiliza para volúmenes persistentes de los pods de vSphere y máquinas virtuales que se ejecutan dentro del Supervisor, y pods de un clúster de Tanzu Kubernetes Grid. Después de crear un Supervisor, como administrador de vSphere puede crear espacios de nombres de vSphere dentro del Supervisor. Como ingeniero de desarrollo y operaciones, puede ejecutar cargas de trabajo que contengan contenedores que se ejecutan dentro de los pods de vSphere, implementar máquinas virtuales a través del servicio de máquina virtual y crear clústeres de Tanzu Kubernetes Grid.

Puede implementar un Supervisor en tres zonas de vSphere para proporcionar alta disponibilidad de nivel de clúster que proteja las cargas de trabajo de Kubernetes contra errores en el nivel de clúster. Una zona de vSphere se asigna a un clúster de vSphere que se puede configurar como un dominio de errores independiente. En una implementación de tres zonas, los tres clústeres de vSphere se convierten en un Supervisor. También puede implementar un Supervisor en un clúster de vSphere, que creará automáticamente una zona de vSphere y la asignará al clúster, a menos que se use un clúster de vSphere que ya esté asignado a una zona. En una implementación de clúster único, el Supervisor solo tiene alta disponibilidad en el nivel de host que proporciona vSphere HA.

Figura 2-2. Arquitectura de Supervisor de tres zonas

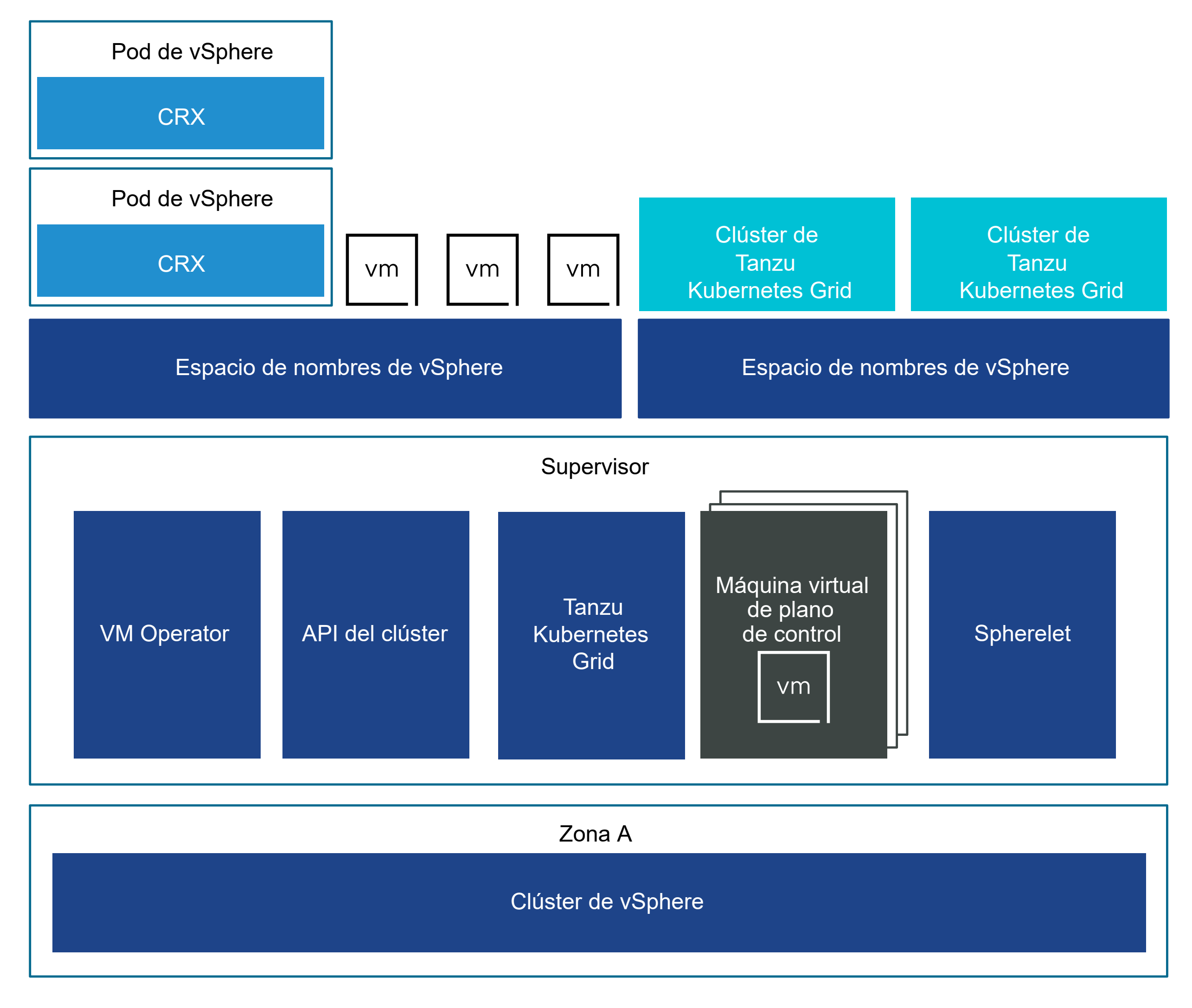


En un Supervisor de tres zonas, puede ejecutar cargas de trabajo de Kubernetes en clústeres de Tanzu Kubernetes Grid y en máquinas virtuales creadas mediante el servicio de máquina virtual. Un Supervisor de tres zonas tiene los siguientes componentes:

- Máquina virtual del plano de control del Supervisor. En total, en el Supervisor se crean tres máquinas virtuales del plano de control del Supervisor. En una implementación de tres zonas, una máquina virtual del plano de control reside en cada zona. Las tres máquinas virtuales del plano de control del Supervisor cuentan con equilibrio de carga, ya que cada una de ellas tiene su propia dirección IP. Además, se asigna una dirección IP flotante a una de las máquinas virtuales y se reserva una 5.ª dirección IP para fines de aplicación de revisiones. vSphere DRS determina la colocación exacta de las máquinas virtuales del plano de control en los hosts ESXi que forman parte del Supervisor y las migra cuando es necesario.
- Tanzu Kubernetes Grid y la API de clúster. Módulos que se ejecutan en el Supervisor y habilitan el aprovisionamiento y la administración de clústeres de Tanzu Kubernetes Grid.
- servicio de máquina virtual. Un módulo que es responsable de implementar y ejecutar las máquinas virtuales independientes y las máquinas virtuales que conforman clústeres de Tanzu Kubernetes Grid.

En un Supervisor de tres zonas se crea un grupo de recursos de espacio de nombres un en cada clúster de vSphere que se asigna a una zona. El espacio de nombres se distribuye entre los tres clústeres de vSphere en cada zona. Los recursos utilizados para el espacio de nombres en un Supervisor de tres zonas se toman de los tres clústeres de vSphere subyacentes a partes iguales. Por ejemplo, si dedica 300 MHz de CPU, se toman 100 MHz de cada clúster de vSphere.

Figura 2-3. Arquitectura de supervisor de clúster único



Un Supervisor implementado en un solo clúster de vSphere también tiene tres máquinas virtuales del plano de control que residen en los hosts ESXi que forman parte del clúster. En un Supervisor de clúster único se pueden ejecutar pods de vSphere además de máquinas virtuales y clústeres de Tanzu Kubernetes Grid. vSphere DRS se integra con el programador de Kubernetes en las máquinas virtuales del plano de control del Supervisor, por lo que DRS determina la colocación de los pods de vSphere. Cuando programa una pod de vSphere como ingeniero de operaciones y desarrollo, la solicitud pasa por el flujo de trabajo de Kubernetes común y después a DRS, el cual toma la decisión de colocación final.

Debido a la compatibilidad con pod de vSphere, un Supervisor de clúster único tiene los siguientes componentes adicionales:

- Spherelet. Se crea un proceso adicional llamado "Spherelet" en cada host. Se trata de un kubelet que se transporta de forma nativa a ESXi y permite que el host ESXi se convierta en parte del clúster de Kubernetes.
- Componente Container Runtime Executive (CRX). CRX es similar a una máquina virtual desde la perspectiva de Hostd y vCenter Server. CRX incluye un kernel de Linux paravirtualizado que funciona junto con el hipervisor. CRX utiliza las mismas técnicas de virtualización de hardware que las máquinas virtuales y tiene un límite de máquina virtual alrededor. Se utiliza una técnica de arranque directo, que permite que el invitado de CRX de Linux inicie el proceso de inicialización principal sin pasar por la inicialización del kernel. Esto permite que los pods de vSphere arranquen casi tan rápido como los contenedores.

Redes del Supervisor

En un entorno de vSphere IaaS control plane, un Supervisor puede utilizar una pila de redes de vSphere o NSX para proporcionar conectividad a las cargas de trabajo, los servicios y las máquinas virtuales del plano de control del Supervisor.

Cuando se configura un Supervisor con la pila de redes de vSphere, todos los hosts del Supervisor se conectan a un vDS que proporciona conectividad a las cargas de trabajo y las máquinas virtuales del plano de control del Supervisor. Un Supervisor que utiliza la pila de redes de vSphere requiere un equilibrador de carga en la red de administración de vCenter Server que proporcione conectividad a los usuarios de desarrollo y operaciones, y a los servicios externos.

Un Supervisor que esté configurado con NSX utiliza las redes basadas en software de la solución, así como un equilibrador de carga de NSX Edge o la NSX Advanced Load Balancer para proporcionar conectividad a los servicios externos y a los usuarios de desarrollo y operaciones. Puede configurar la NSX Advanced Load Balancer en NSX si el entorno cumple las siguientes condiciones:

- La versión de NSX es 4.1.1 o posterior.
- La versión de NSX Advanced Load Balancer es la 22.1.4 o posterior con la licencia Enterprise.
- La NSX Advanced Load Balancer Controller que tiene pensado configurar se registra en NSX.
- Aún no se ha configurado un equilibrador de carga de NSX en el Supervisor.

Redes de un Supervisor con VDS

En un Supervisor respaldado por VDS como la pila de redes, todos los hosts de los clústeres de vSphere que respaldan el Supervisor deben estar conectados al mismo VDS. El Supervisor utiliza grupos de puertos distribuidos como redes de carga de trabajo para el tráfico del plano de control y las cargas de trabajo de Kubernetes. Las redes de carga de trabajo se asignan a los espacios de nombres en el Supervisor.

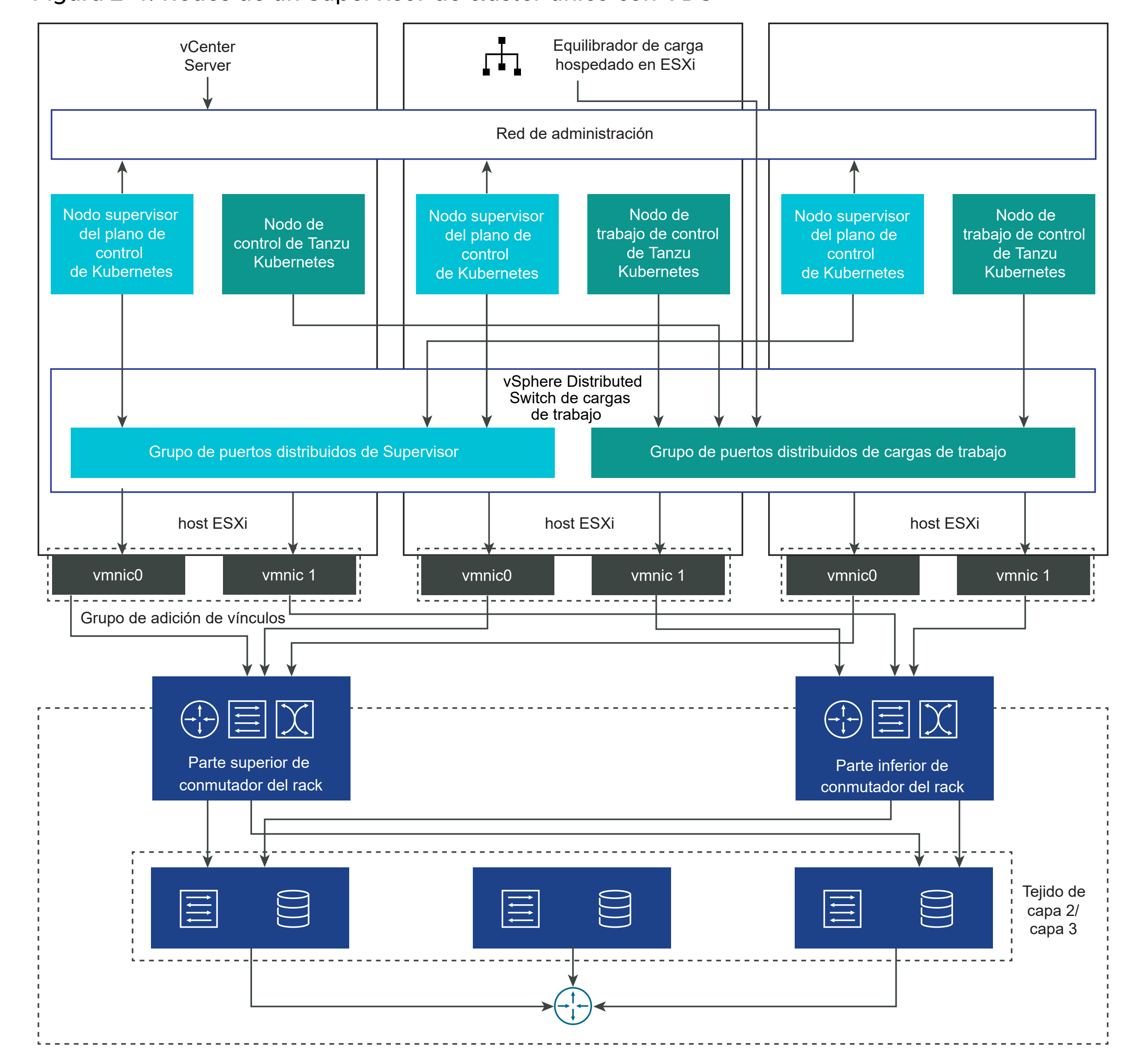
Según la topología que se implemente para el Supervisor, es posible usar uno o varios grupos de puertos distribuidos como redes de carga de trabajo. La red que proporciona conectividad a las máquinas virtuales del plano de control del Supervisor se denomina Red de carga de trabajo principal. Puede asignar esta red a todos los espacios de nombres de la instancia de Supervisor o puede utilizar diferentes redes para cada espacio de nombres. Los clústeres de Tanzu Kubernetes Grid se conectan a la red de carga de trabajo que se asigna al espacio de nombres en el que residen los clústeres.

Un Supervisor respaldado por un VDS utiliza un equilibrador de carga para proporcionar conectividad a los usuarios de desarrollo y operaciones, y a los servicios externos. Puede utilizar el NSX Advanced Load Balancer o el equilibrador de carga de HAProxy.

Para obtener más información, consulte Instalar y configurar NSX Advanced Load Balancer e Instalar y configurar el equilibrador de carga de HAProxy.

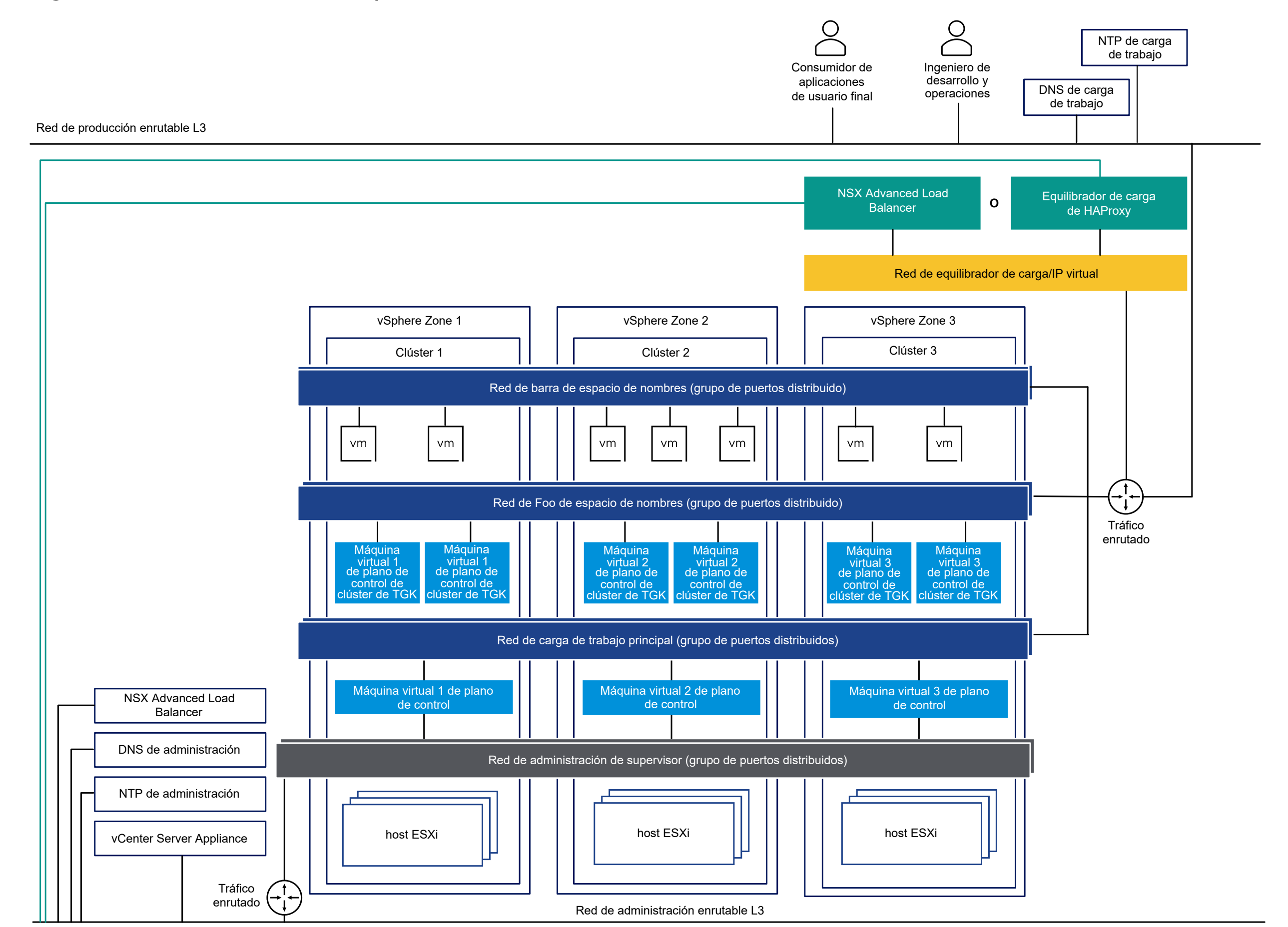
En una configuración de Supervisor de clúster único, el Supervisor está respaldado por un solo clúster de vSphere. Todos los hosts del clúster deben estar conectados a un VDS.

Figura 2-4. Redes de un Supervisor de clúster único con VDS



En un Supervisor de tres zonas, se implementa el Supervisor en tres zonas de vSphere, cada una asignada a un clúster de vSphere. Todos los hosts de estos clústeres de vSphere deben estar conectados al mismo VDS. Todos los servidores físicos deben estar conectados a un dispositivo de capa 2. Las redes de carga de trabajo que se configuran en el espacio de nombres abarcan las tres zonas de vSphere.

Figura 2-5. Redes de un Supervisor de tres zonas con VDS



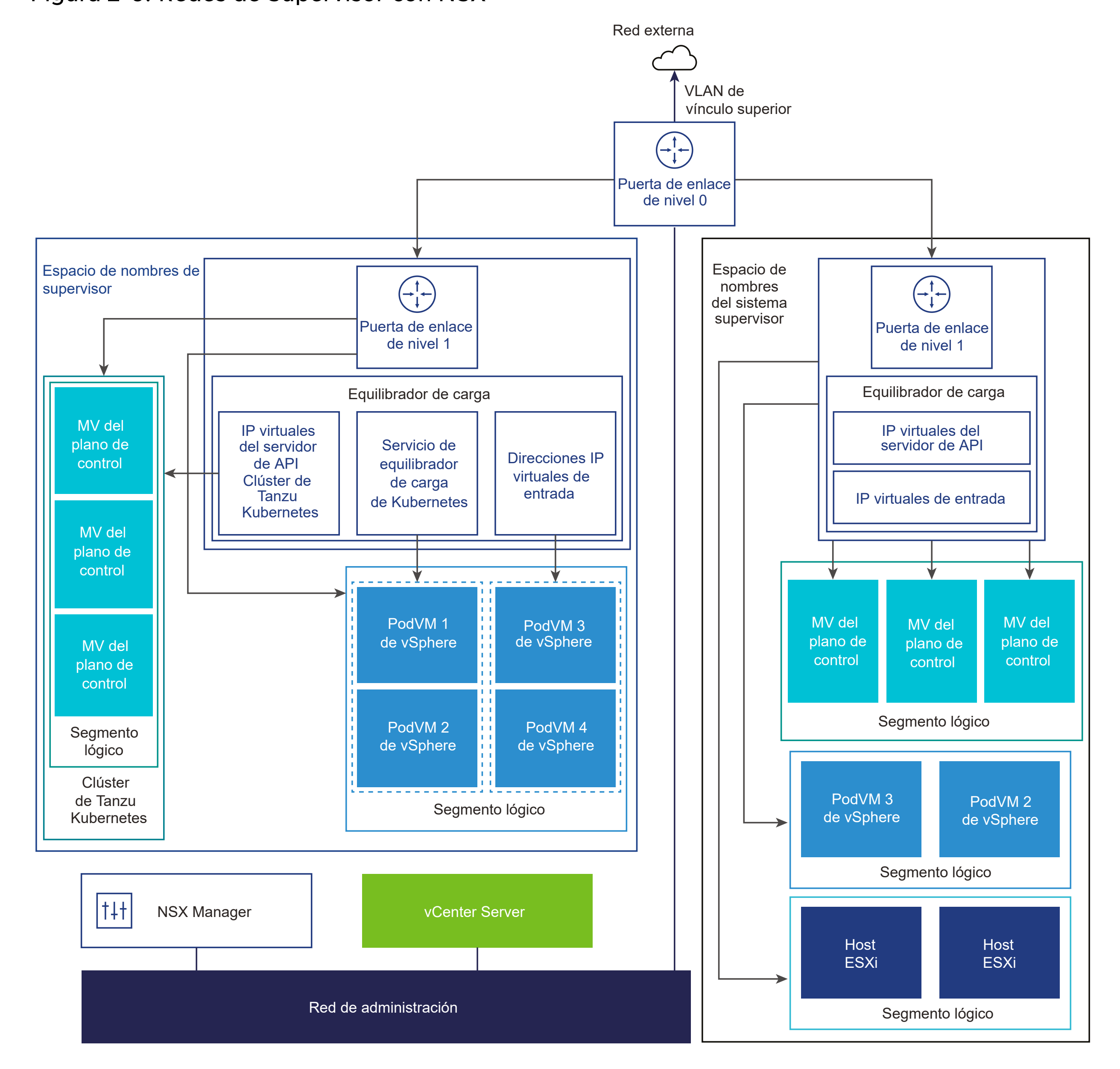
Redes de Supervisor con NSX

NSX proporciona conectividad de red a los objetos dentro de Supervisor y las redes externas. La conectividad con los hosts ESXi que componen el clúster se gestiona mediante las redes vSphere estándar.

También puede configurar manualmente las redes de Supervisor mediante una implementación de NSX existente o mediante la implementación de una nueva instancia de NSX.

Para obtener más información, consulte Instalar y configurar NSX para vSphere IaaS control plane.

Figura 2-6. Redes de Supervisor con NSX



- NSX Container Plugin (NCP) proporciona integración entre NSX y Kubernetes. El componente principal de NCP se ejecuta en un contenedor y se comunica con NSX Manager y con el plano de control de Kubernetes. NCP supervisa los cambios en los contenedores y otros recursos, y administra los recursos de redes, como los puertos lógicos, los segmentos, los enrutadores y los grupos de seguridad de los contenedores mediante una llamada a NSX API.

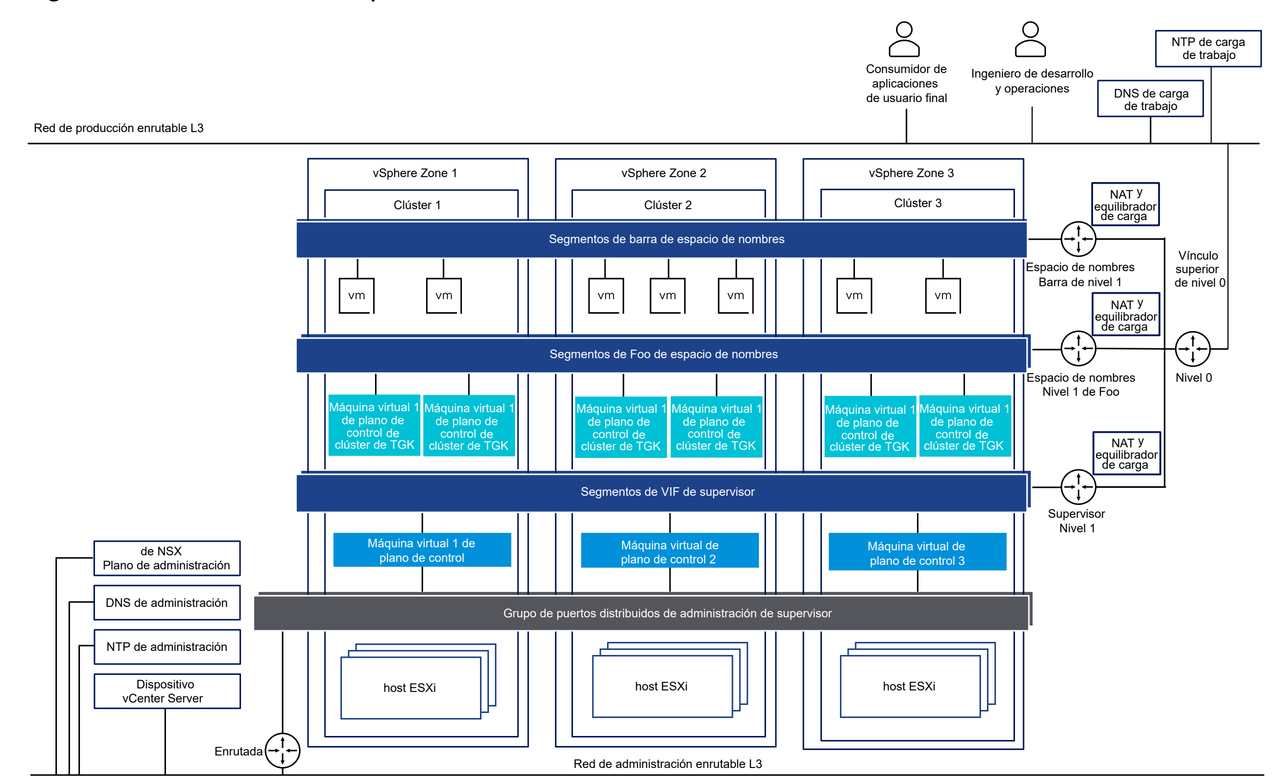
  NCP crea de forma predeterminada una puerta de enlace de nivel 1 compartida para los espacios de nombres del sistema y una puerta de enlace de nivel 1 y un equilibrador de carga para cada espacio de nombres. La puerta de enlace de nivel 1 está conectada a la puerta de enlace de nivel 0 y a un segmento predeterminado.

Los espacios de nombres del sistema son espacios de nombres utilizados por los componentes principales que son esenciales para el funcionamiento de los clústeres de Supervisor y de Tanzu Kubernetes Grid. Los recursos de red compartidos que incluyen la puerta de enlace de nivel 1, el equilibrador de carga y la IP de SNAT se agrupan en un espacio de nombres del sistema.

- NSX Edge proporciona conectividad de redes externas a objetos del Supervisor. El clúster de NSX Edge tiene un equilibrador de carga que proporciona redundancia a los servidores de API de Kubernetes que residen en las máquinas virtuales del plano de control del Supervisor, así como en cualquier aplicación que deba publicarse y a la que se pueda acceder desde fuera del Supervisor.
- Se asocia una puerta de enlace de nivel 0 al clúster de NSX Edge para proporcionar enrutamiento a la red externa. La interfaz de vínculo superior utiliza el protocolo de enrutamiento dinámico, BGP o enrutamiento estático.
- Cada espacio de nombres de vSphere tiene una red independiente y un conjunto de recursos de red compartidos por las aplicaciones que están dentro del espacio de nombres, como la puerta de enlace de nivel 1, el servicio de equilibrador de carga y la dirección IP de SNAT.
- Las cargas de trabajo que se ejecutan en pods de vSphere, máquinas virtuales normales o clústeres de Tanzu Kubernetes Grid, los cuales están en el mismo espacio de nombres, comparten una misma IP de SNAT para la conectividad de norte a sur.
- Las cargas de trabajo que se ejecutan en clústeres de pods de vSphere o Tanzu Kubernetes Grid tendrán la misma regla de aislamiento que implementa el firewall predeterminado.
- No se requiere una IP de SNAT independiente para cada espacio de nombres de Kubernetes. La conectividad de este a oeste entre espacios de nombres no será SNAT.
- Los segmentos de cada espacio de nombres residen en la instancia de VDS que funciona en el modo estándar y está asociada con el clúster de NSX Edge. El segmento proporciona una red de superposición al Supervisor.
- Los Supervisores tienen segmentos separados dentro de la puerta de enlace de nivel 1 compartida. Para cada clúster de Tanzu Kubernetes Grid, los segmentos se definen en la puerta de enlace de nivel 1 del espacio de nombres.
- Los procesos de Spherelet en cada host ESXi se comunican con vCenter Server a través de una interfaz de la red de administración.

En un Supervisor de tres zonas configurado con NSX como pila de redes, todos los hosts de los tres clústeres de vSphere asignados a las zonas deben estar conectados al mismo VDS y participar en la misma zona de transporte superpuesta de NSX. Todos los hosts deben estar conectados al mismo dispositivo físico de capa 2.

Figura 2-7. Redes de un Supervisor de tres zonas con NSX



Redes de Supervisor con NSX y NSX Advanced Load Balancer

NSX proporciona conectividad de red a los objetos dentro de Supervisor y las redes externas. Un Supervisor que esté configurado con NSX puede utilizar NSX Edge o NSX Advanced Load Balancer.

Los componentes de NSX Advanced Load Balancer incluyen el clúster de la NSX Advanced Load Balancer Controller, las máquinas virtuales de los motores de servicio (plano de datos) y el operador de AVI Kubernetes (AKO).

La NSX Advanced Load Balancer Controller interactúa con vCenter Server para automatizar el equilibrio de carga de los clústeres de Tanzu Kubernetes Grid. Se encarga de aprovisionar los motores de servicio, coordinar los recursos entre los motores de servicio y agregar métricas y registros de los motores de servicio. La controladora proporciona una interfaz web, una interfaz de línea de comandos y una API para el funcionamiento del usuario y la integración programática. Después de implementar y configurar la máquina virtual de la controladora, puede implementar un clúster de la controladora para configurar el clúster del plano de control para HA.

El motor de servicio es la máquina virtual del plano de datos. Un motor de servicio ejecuta uno o varios servicios virtuales. La NSX Advanced Load Balancer Controller administra un motor de servicio. La controladora aprovisiona los motores de servicio para alojar servicios virtuales.

El motor de servicio tiene dos tipos de interfaces de red:

- La primera interfaz de red, `vnic0` de la máquina virtual, se conecta a la red de administración, donde puede conectarse a la NSX Advanced Load Balancer Controller.

- Las restantes interfaces, `vnic1 - 8`, se conectan a la red de datos en la que se ejecutan los servicios virtuales.

Las interfaces del motor de servicio se conectan automáticamente a los grupos de puertos de vDS correctos. Cada motor de servicio puede admitir hasta 1000 servicios virtuales.

Un servicio virtual proporciona servicios de equilibrio de carga de capa 4 y capa 7 para cargas de trabajo del clúster de Tanzu Kubernetes Grid. Un servicio virtual se configura con una IP virtual y varios puertos. Cuando se implementa un servicio virtual, el controlador selecciona automáticamente una instancia de ESX Server, aumenta la velocidad de giro de un motor de servicio y lo conecta a las redes correctas (grupos de puertos).

El primer motor de servicio solo se crea después de configurar el primer servicio virtual. Todos los servicios virtuales que se configuren posteriormente utilizarán el motor de servicio existente.

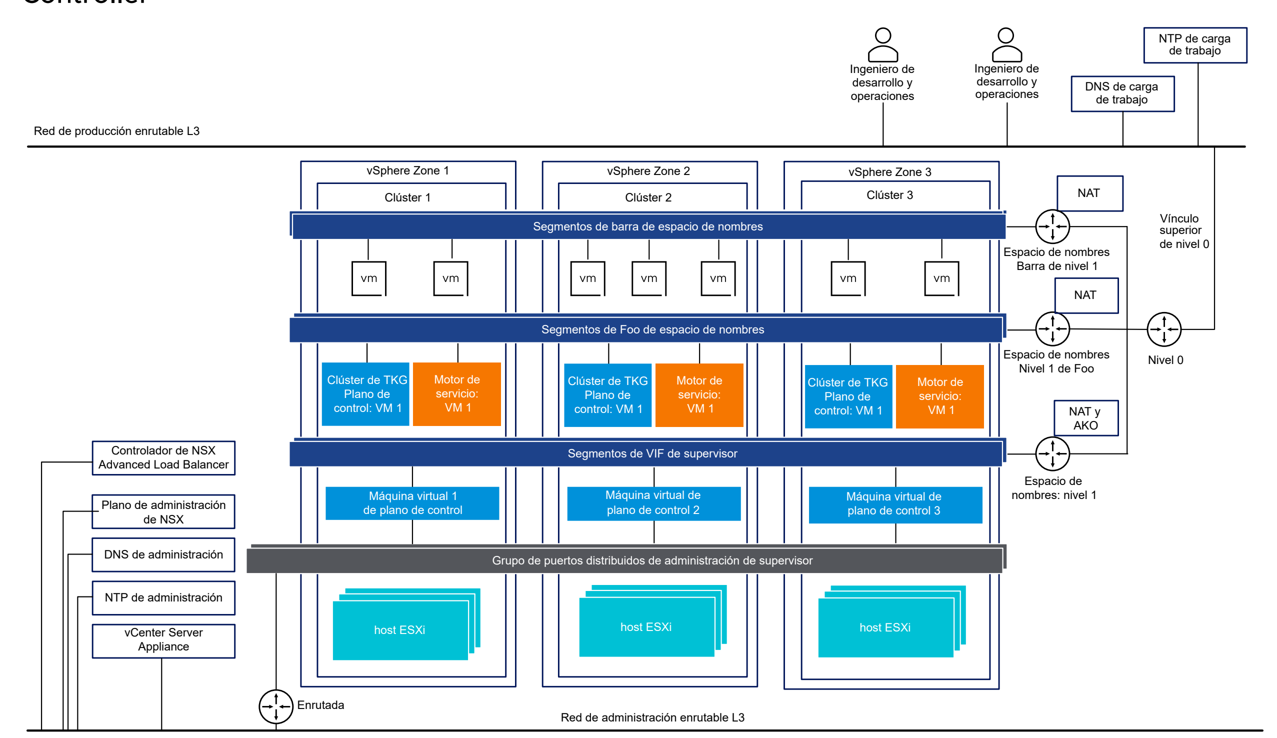
Cada servidor virtual expone un equilibrador de carga de capa 4 con una dirección IP distinta del tipo equilibrador de carga para un clúster de Tanzu Kubernetes Grid. La dirección IP asignada a cada servidor virtual se selecciona en el bloque de direcciones IP otorgado a la controladora cuando se configura.

El operador de AVI Kubernetes (AKO) consulta los recursos de Kubernetes y se comunica con la NSX Advanced Load Balancer Controller para solicitar los recursos de equilibrio de carga correspondientes. El operador de AVI Kubernetes se instala en los Supervisores como parte del proceso de habilitación.

Para obtener más información, consulte Instalar y configurar NSX y NSX Advanced Load Balancer.

Figura 2-8. Redes de Supervisor con NSX y NSX Advanced Load Balancer Controller

Figura 2-9. Redes de un Supervisor de tres zonas con NSX y NSX Advanced Load Balancer Controller



Importante Cuando configure la NSX Advanced Load Balancer Controller en una implementación de NSX, tenga en cuenta las siguientes consideraciones:

- No se puede implementar la NSX Advanced Load Balancer Controller en una implementación de Enhanced Linked Mode de vCenter Server. Solo se puede implementar la NSX Advanced Load Balancer Controller en una única implementación de vCenter Server. Si hay más de una instancia de vCenter Server vinculada, solo se puede utilizar una de ellas al configurar la NSX Advanced Load Balancer Controller.
- No se puede configurar la NSX Advanced Load Balancer Controller en una topología de nivel 0 de varios niveles. Si el entorno de NSX está configurado con una topología de nivel 0 de varios niveles, solo se puede utilizar una puerta de enlace de nivel 0 mientras configura la NSX Advanced Load Balancer Controller.

Métodos de configuración de redes con NSX

El Supervisor usa una configuración de redes taxativa. Existen dos métodos para configurar las redes del Supervisor con NSX que dan como resultado la implementación del mismo modelo de redes para un Supervisor de una zona:

- La forma más sencilla de configurar las redes de Supervisor es mediante VMware Cloud Foundation SDDC Manager. Para obtener más información, consulte la documentación de VMware Cloud Foundation SDDC Manager. Para obtener más información, consulte Guía de administración de VMware Cloud Foundation.

- También puede configurar manualmente las redes de Supervisor mediante una implementación de NSX existente o mediante la implementación de una nueva instancia de NSX. Para obtener más información, consulte Instalar y configurar NSX para vSphere IaaS control plane.

Almacenamiento de Supervisor

Los componentes, las aplicaciones y las cargas de trabajo del Supervisor necesitan almacenar y recuperar datos. Algunas aplicaciones y objetos pueden utilizar almacenamiento rápido transitorio, mientras que otros requieren un almacenamiento persistente.

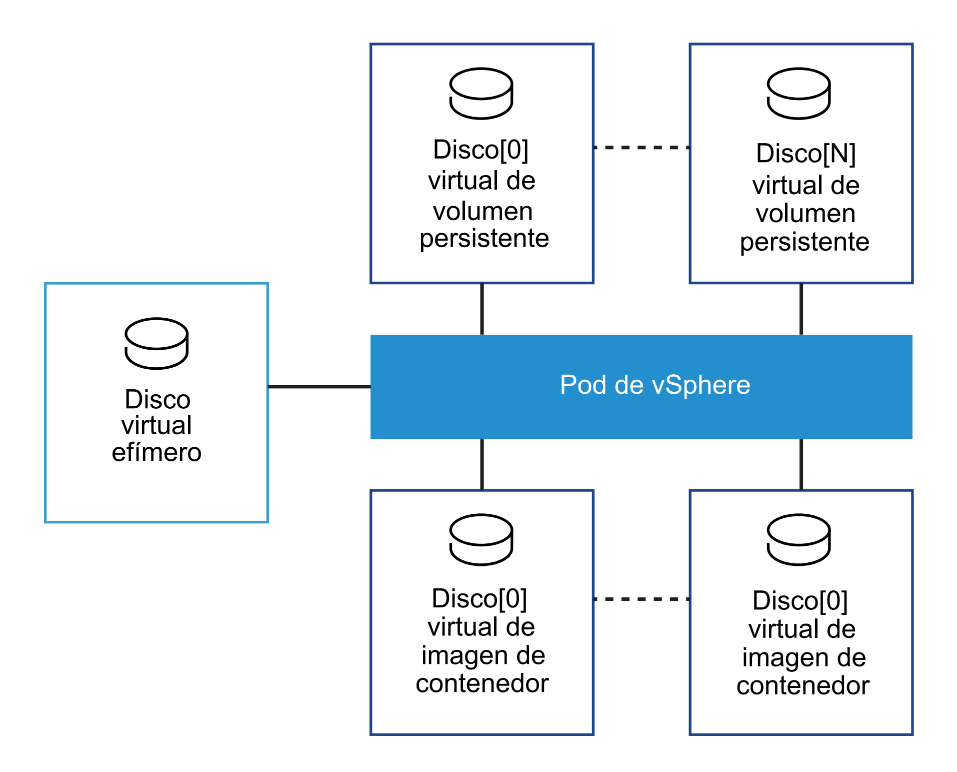
Acerca de las directivas de almacenamiento

El Supervisor utiliza directivas de almacenamiento para integrarse con el almacenamiento disponible en el entorno de vSphere. Las directivas representan almacenes de datos y administran la colocación del almacenamiento de componentes y objetos como máquinas virtuales del plano de control, discos efímeros de pod de vSphere e imágenes de contenedor. Es posible que también necesite directivas para la colocación del almacenamiento de los volúmenes persistentes y las bibliotecas de contenido de máquina virtual. Si utiliza clústeres de Tanzu Kubernetes Grid, las directivas de almacenamiento también determinan cómo se implementan los nodos del clúster de Tanzu Kubernetes Grid.

Las directivas de almacenamiento admiten cualquier almacén de datos compartido en su entorno, como VMFS, NFS, vSAN, incluido vSAN ESA, o vVols.

Según el entorno de almacenamiento de vSphere y las necesidades de desarrollo y operaciones, puede crear varias directivas de almacenamiento para diferentes clases de almacenamiento. Cuando se habilita un Supervisor y se configuran espacios de nombres, es posible asignar diferentes directivas de almacenamiento para que las utilicen diversos objetos, componentes y cargas de trabajo.

Por ejemplo, si un pod de vSphere monta tres tipos de discos virtuales y su entorno de almacenamiento de vSphere tiene tres clases de almacenes de datos (Bronce, Plata y Oro), puede crear directivas de almacenamiento para todos los almacenes de datos. Posteriormente, puede utilizar el almacén de datos Bronce para los discos virtuales efímeros y los discos virtuales de imagen de contenedor, y utilizar los almacenes de datos Plata y Oro para los discos virtuales de volumen persistente.



Para obtener información sobre la creación de directivas de almacenamiento, consulte Crear directivas de almacenamiento en la documentación de *Instalar y configurar el plano de control de IaaS de vSphere*.

Para obtener información general acerca de las directivas de almacenamiento, consulte el capítulo Administración basada en directiva de almacenamiento en la documentación de *Almacenamiento de vSphere*.

Directivas de almacenamiento para un Supervisor

En el nivel del Supervisor se configura una directiva de almacenamiento para las máquinas virtuales del plano de control del Supervisor. Además, si la implementación admite pods de vSphere, asigne directivas de almacenamiento y especifique las ubicaciones de los almacenes de datos para los discos efímeros y las imágenes de contenedor. Para obtener información sobre la configuración de las directivas de almacenamiento cuando se habilita el Supervisor, consulte la documentación *Instalar y configurar el plano de control de IaaS de vSphere*. Para cambiar la configuración de almacenamiento, consulte Cambiar la configuración de almacenamiento en el Supervisor.

Directiva de almacenamiento del plano de control

Esta directiva garantiza que las máquinas virtuales del plano de control se coloquen en los almacenes de datos que representan las directivas.

Discos virtuales efímeros

Una pod de vSphere requiere almacenamiento efímero para almacenar objetos de Kubernetes como registros, volúmenes de `emptyDir` y `ConfigMaps` durante sus operaciones.

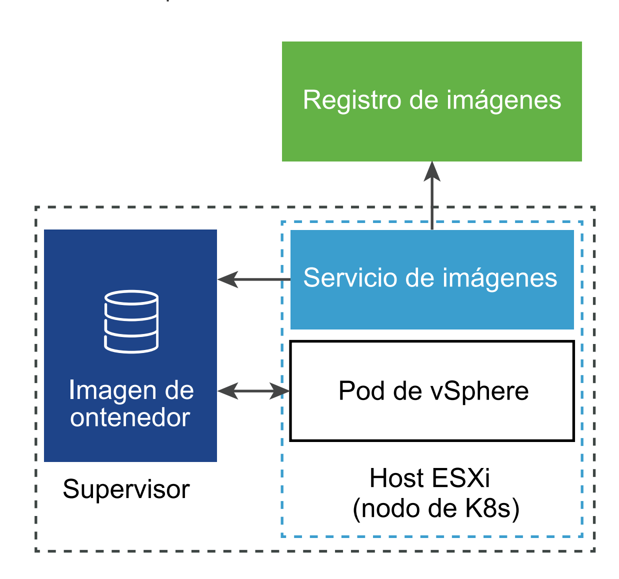
Este almacenamiento efímero, o transitorio, dura mientras que el pod siga existiendo. Los datos efímeros se conservan entre los reinicios del contenedor, pero una vez que el pod llega al final de su vida, el disco virtual efímero desaparece.

Cada pod tiene un disco virtual efímero. Como administrador de vSphere, usted utiliza una directiva de almacenamiento para definir la ubicación del almacén de datos de todos los discos virtuales efímeros al configurar el almacenamiento para el Supervisor.

Discos virtuales de imagen de contenedor

Los contenedores dentro de la pod de vSphere utilizan imágenes que contienen el software que se ejecutará. El pod monta imágenes utilizadas por sus contenedores como discos virtuales de imagen. Cuando el pod completa su ciclo de vida, los discos virtuales de imagen se desasocian del pod.

El servicio de imágenes, un componente de ESXi, es responsable de extraer imágenes de contenedor del registro de imágenes y transformarlas en discos virtuales para ejecutarlas dentro del pod.



ESXi puede almacenar en la memoria caché las imágenes descargadas para los contenedores que se ejecutan en el pod. Los pods subsiguientes que utilizan la misma imagen la extraen de la memoria caché local en lugar del registro de contenedor externo.

Almacenamiento persistente para cargas de trabajo

Ciertas cargas de trabajo de Kubernetes que desarrollo y operaciones ejecutan en un espacio de nombres requieren almacenamiento persistente para almacenar datos de forma permanente.

El almacenamiento persistente puede ser utilizado por pods de vSphere, clústeres de Tanzu Kubernetes Grid, máquinas virtuales y otras cargas de trabajo que se ejecutan en el espacio de nombres. Para que el almacenamiento persistente esté disponible para el equipo de desarrollo y operaciones, el administrador de vSphere crea directivas de almacenamiento que describen distintos requisitos de almacenamiento y clases de servicios. Después el administrador asigna directivas de almacenamiento y configura los límites de almacenamiento en un nivel de espacio de nombres.

Para comprender cómo funciona vSphere IaaS control plane con almacenamiento persistente, familiarícese con los conceptos esenciales de Kubernetes, como las clases de almacenamiento, los volúmenes persistentes y las notificaciones de volúmenes persistentes. Para obtener más información, consulte la documentación de Kubernetes en https://kubernetes.io/docs/home/.

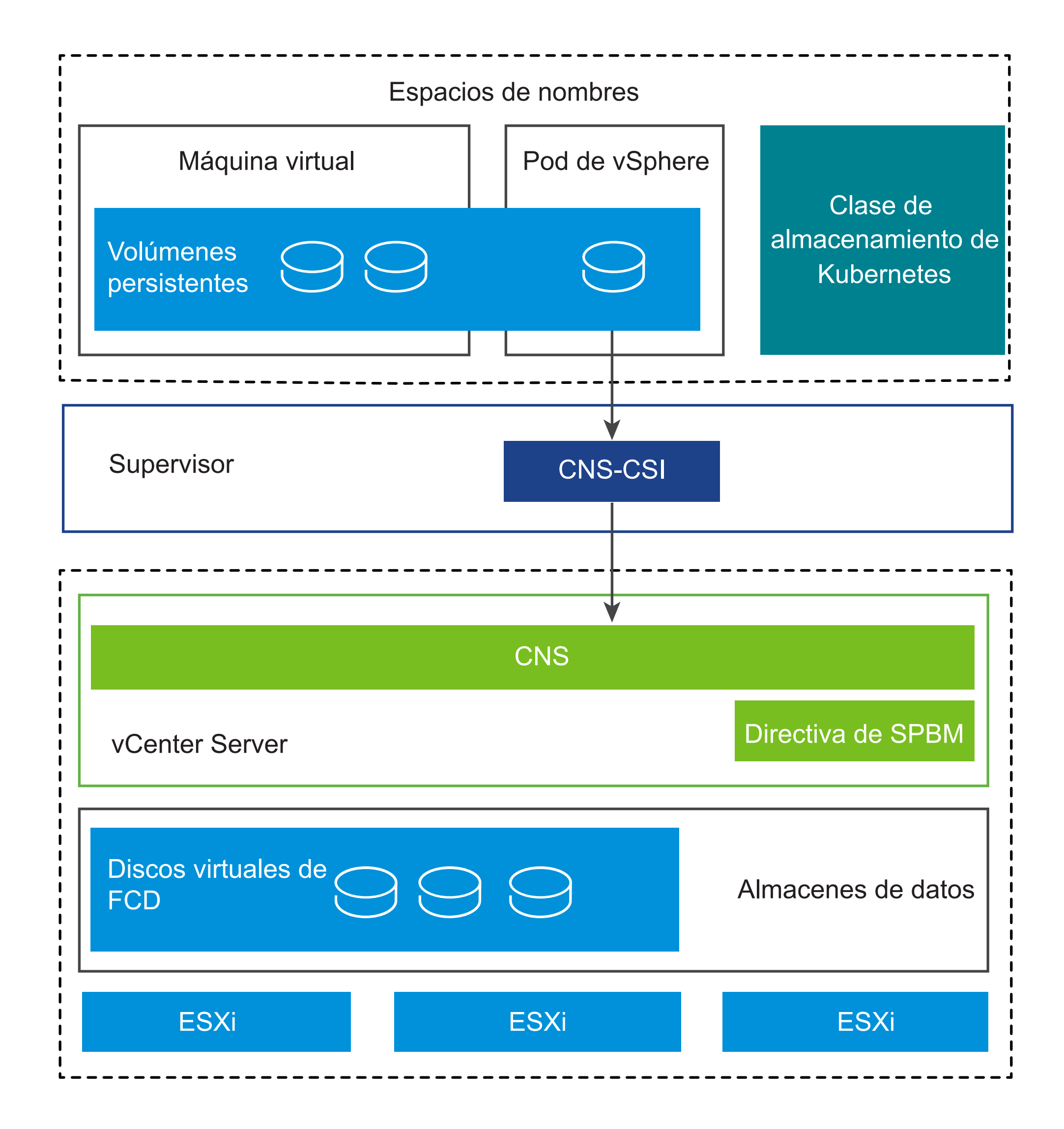
Para obtener información sobre el almacenamiento persistente para un clúster de Tanzu Kubernetes Grid, consulte Almacenamiento para clústeres de Tanzu Kubernetes Grid.

Para obtener información sobre el uso del almacenamiento persistente, consulte Uso del almacenamiento persistente con cargas de trabajo en la documentación de *Servicios y cargas de trabajo del plano de control de IaaS de vSphere*.

Si el equipo de desarrollo y operaciones planea implementar servicios de terceros que utilizan vSAN Direct para sus necesidades de almacenamiento persistente, consulte Habilitar servicios con estado en vSphere con Tanzu en la documentación de *Servicios y cargas de trabajo del plano de control de IaaS de vSphere*.

Cómo se integra Supervisor con el almacenamiento de vSphere

Supervisor utiliza varios componentes para integrarse con el almacenamiento de vSphere.



Almacenamiento nativo en la nube (CNS) en vCenter Server

El componente CNS reside en vCenter Server. Se trata de una extensión de administración de vCenter Server que implementa las operaciones de aprovisionamiento y ciclo de vida de los volúmenes persistentes.

Cuando se aprovisionan volúmenes persistentes, el componente interactúa con la funcionalidad de disco de primera clase de vSphere para crear discos virtuales que respaldan esos volúmenes. Adicionalmente, el componente de servidor de almacenamiento nativo en la nube se comunica con la administración de almacenamiento basada en directivas para garantizar un nivel necesario de servicio a los discos.

El almacenamiento nativo en la nube también realiza operaciones de consulta que permiten a los administradores de vSphere administrar y supervisar volúmenes persistentes y sus objetos de almacenamiento de respaldo a través de vCenter Server.

Disco de primera clase (First Class Disk, FCD)

También se denomina disco virtual mejorado. Estos discos residen en almacenes de datos y respaldan volúmenes persistentes ReadWriteOnce.

Al usar FCD, tenga en cuenta lo siguiente:

- Los FCD no admiten protocolos NFS 4.x. En su lugar, utilice NFS 3.
- vCenter Server no serializa las operaciones en el mismo FCD. Como resultado, las aplicaciones no pueden realizar operaciones simultáneamente en el mismo FCD. Realizar operaciones, tales como clonar, reubicar, eliminar, recuperar, etc., al mismo tiempo desde diferentes subprocesos provoca resultados impredecibles. Para evitar problemas, las aplicaciones deben realizar operaciones en el mismo FCD en un orden secuencial.
- FCD no es un objeto administrado y no admite un bloqueo global que proteja varias escrituras en un único FCD. Como resultado, FCD no admite varias instancias de vCenter Server que administren el mismo FCD. Si necesita utilizar varias instancias de vCenter Server con FCD, tiene las siguientes opciones:
  - Varias instancias de vCenter Server pueden administrar distintos almacenes de datos.
  - Varias instancias de vCenter Server no funcionan en el mismo FCD.

Administración de almacenamiento basada en directivas

La administración de almacenamiento basada en directivas es un servicio del vCenter Server que admite el aprovisionamiento de volúmenes persistentes y sus discos virtuales de respaldo según los requisitos de almacenamiento descritos en una directiva de almacenamiento. Después del aprovisionamiento, el servicio supervisa el cumplimiento del volumen con las características de directiva de almacenamiento. Para obtener más información sobre la administración de almacenamiento basada en directivas, consulte el capítulo Administración de almacenamiento basada en directivas de la documentación de *Almacenamiento de vSphere*.

CNS-CSI de vSphere

El componente CNS-CSI de vSphere cumple con la especificación de la interfaz de almacenamiento de contenedor (Container Storage Interface, CSI), un estándar de la industria diseñado para proporcionar una interfaz que los orquestadores de contenedores como Kubernetes utilizan para aprovisionar el almacenamiento persistente. El controlador de CNS-CSI se ejecuta en el Supervisor y conecta el almacenamiento de vSphere al entorno de Kubernetes en un espacio de nombres. CNS-CSI de vSphere se comunica directamente con el componente de CNS para todas las solicitudes de aprovisionamiento de almacenamiento que se originan desde el espacio de nombres.

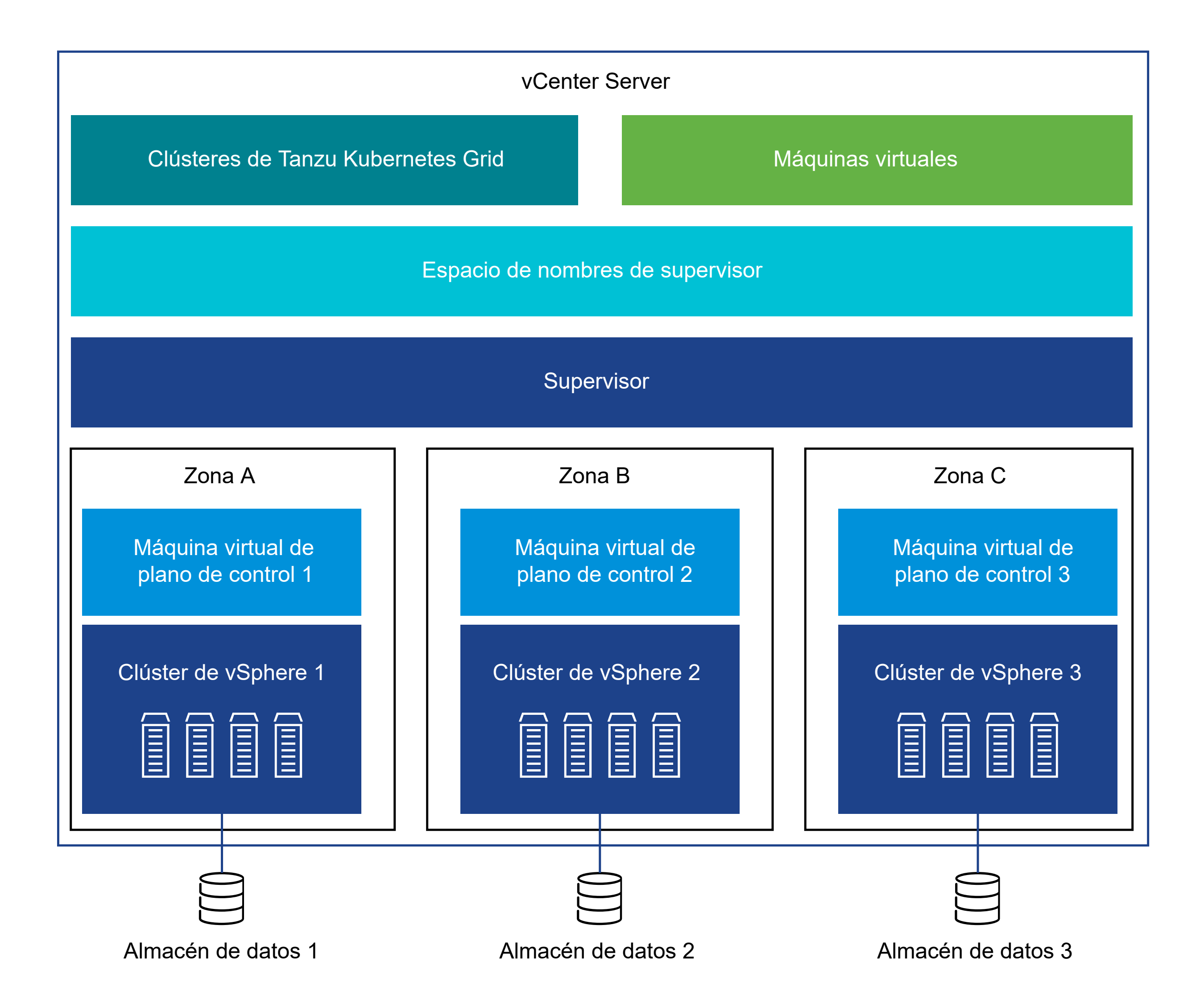
Funcionalidad admitida por vSphere CNS-CSI

El componente CNS-CSI de vSphere que se ejecuta en el Supervisor admite varias funciones de almacenamiento de vSphere y Kubernetes. No obstante, se aplican algunas limitaciones.

Funcionalidades admitidas	CNS-CSI de vSphere con Supervisor
Compatibilidad de CNS en vSphere Client	Sí
Estado mejorado del objeto en vSphere Client	Sí (solo vSAN)
Volumen persistente de bloques dinámicos (modo de acceso ReadWriteOnce)	Sí
Volumen persistente de archivos dinámicos (modo de acceso ReadWriteMany)	No
Almacén de datos de vSphere	VMFS, NFS, vSAN (incluido vSAN ESA), vVols
Volumen persistente estático	Sí
Cifrado	No
Expansión de volumen sin conexión	Sí
Expansión de volumen conectado	Sí
Topologías de volumen y zonas	Sí. Los volúmenes solo los pueden consumir clústeres de Tanzu Kubernetes Grid.
Varias instancias del plano de control de Kubernetes	Sí
WaitForFirstConsumer	No
VolumeHealth	Sí
Storage vMotion con volúmenes persistentes	No

Almacenamiento persistente y Supervisor con zonas de vSphere

Un Supervisor de tres zonas admite el almacenamiento de zonas, donde un almacén de datos se comparte entre todos los hosts de una sola zona.



Cuando prepare recursos de almacenamiento para el Supervisor de tres zonas, tenga en cuenta las siguientes consideraciones:

- No es necesario que el almacenamiento de las tres zonas sea del mismo tipo. Sin embargo, tener un almacenamiento uniforme en los tres clústeres proporciona un rendimiento coherente.
- Para el espacio de nombres en el Supervisor de tres zonas, utilice una directiva de almacenamiento que sea compatible con el almacenamiento compartido en cada uno de los clústeres. La directiva de almacenamiento debe tener reconocimiento de topología.
- No elimine las restricciones de topología de la directiva de almacenamiento después de asignarla al espacio de nombres.
- No monte almacenes de datos de zonas en otras zonas.
- Un Supervisor de tres zonas no admite los siguientes elementos:
  - Volúmenes entre zonas

- Volúmenes de archivos de vSAN (volúmenes ReadWriteMany)
- Aprovisionamiento de volúmenes estáticos mediante la API de registrar volumen
- Cargas de trabajo que utilizan la plataforma de persistencia de datos de vSAN
- pod de vSphere
- Clústeres ampliados de vSAN
- Máquinas virtuales con vGPU y almacenamiento de instancias

Para obtener más información, consulte Usar almacenamiento persistente en un supervisor de tres zonas en la documentación de *Servicios y cargas de trabajo del plano de control de IaaS de vSphere*.

Arquitectura y componentes del Tanzu Kubernetes Grid

3

Compruebe cuál es la arquitectura de Tanzu Kubernetes Grid y cómo se integra con el Supervisor y sus componentes. Conozca cómo funcionan las redes y el almacenamiento para los clústeres de Tanzu Kubernetes Grid, así como qué es alta disponibilidad para Tanzu Kubernetes Grid y qué implementación del Supervisor la admite.

Lea los siguientes temas a continuación:

Arquitectura del Tanzu Kubernetes Grid

Tanzu Kubernetes Grid proporciona la administración del ciclo de vida de autoservicio de los clústeres de Tanzu Kubernetes Grid. Puede usar Tanzu Kubernetes Grid a fin de crear y administrar los clústeres de Tanzu Kubernetes Grid de una forma declarativa que es conocida para los operadores y los desarrolladores de Kubernetes.

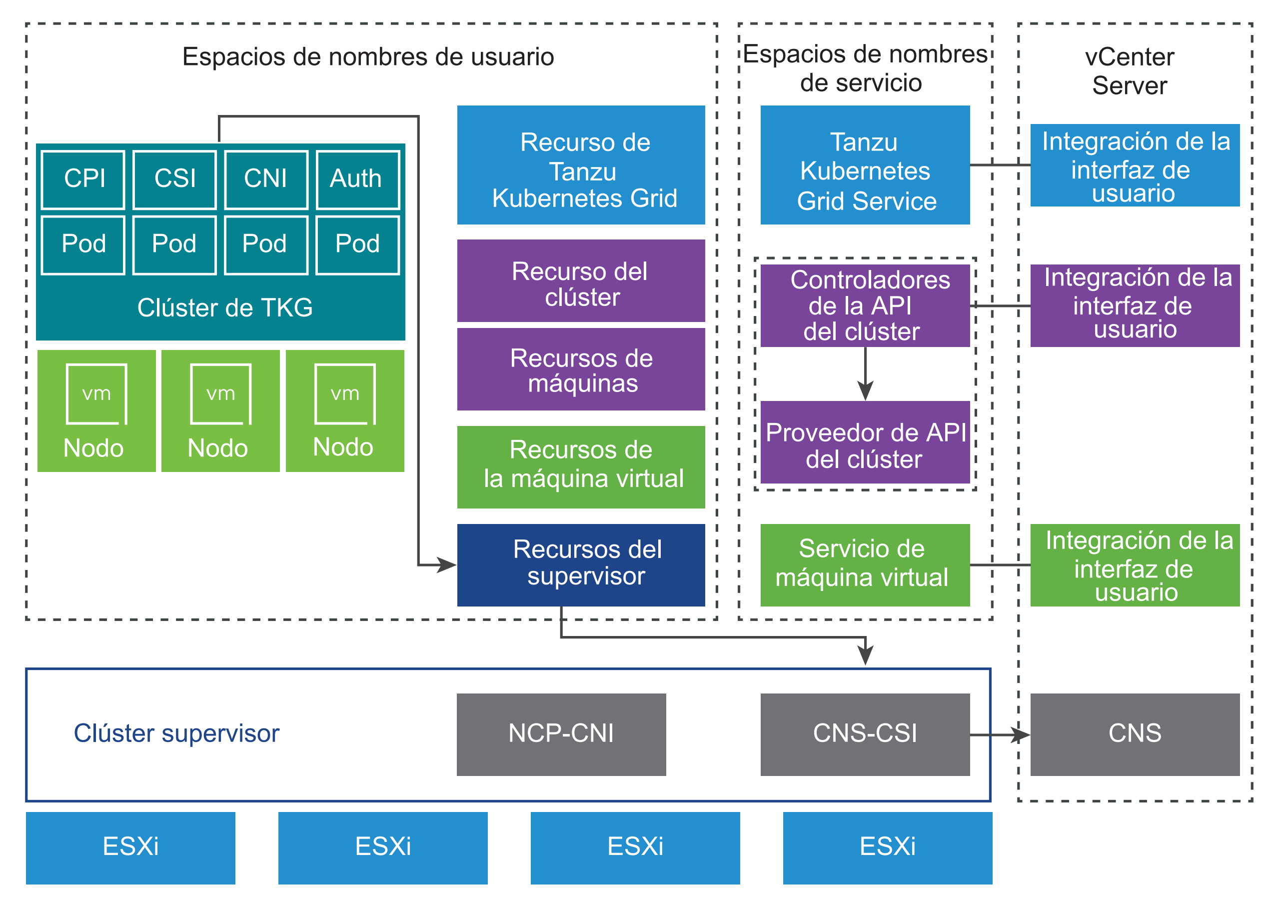
Componentes de Tanzu Kubernetes Grid

Tanzu Kubernetes Grid expone tres capas de controladoras para administrar el ciclo de vida de un clúster de Tanzu Kubernetes Grid.

- Tanzu Kubernetes Grid aprovisiona clústeres que incluyen los componentes necesarios para la integración con los recursos subyacentes de espacio de nombres de vSphere. Estos componentes incluyen un complemento de proveedor de nube que se integra con la instancia de Supervisor. Asimismo, un clúster de Tanzu Kubernetes Grid envía solicitudes de volúmenes persistentes a Supervisor, que se integra con el almacenamiento nativo en la nube (Cloud Native Storage, CNS) de VMware. Consulte Almacenamiento persistente para cargas de trabajo.

- La API del clúster proporciona API de estilo Kubernetes declarativas para la creación, la configuración y la administración del clúster. Las entradas de la API del clúster incluyen un recurso que describe el clúster, un conjunto de recursos que describen las máquinas virtuales que componen el clúster y un conjunto de recursos que describen los complementos del clúster.
- El servicio de máquina virtual proporciona una API declarativa estilo Kubernetes para la administración de las máquinas virtuales y los recursos de vSphere asociados. El servicio de máquina virtual presenta el concepto de una clase de máquina virtual que representa una configuración de hardware reutilizable y abstracta. La funcionalidad que el servicio de máquina virtual proporciona se utiliza para administrar el ciclo de vida de las máquinas virtuales del plano de control y del nodo de trabajo que alojan un clúster de Tanzu Kubernetes Grid.

Figura 3-1. Arquitectura y componentes del Tanzu Kubernetes Grid



Componentes del clúster de Tanzu Kubernetes Grid

Los componentes que se ejecutan en un clúster de Tanzu Kubernetes Grid abarcan cuatro áreas: autenticación y autorización, integración de almacenamiento, redes de pod, y equilibrio de carga.

- Webhook de autenticación: un webhook que se ejecuta como pod dentro del clúster para validar los tokens de autenticación de usuario.

- Complemento de interfaz de almacenamiento de contenedor: un complemento de CSI paravirtual que se integra con CNS a través de Supervisor.
- Complemento de interfaz de redes de contenedor: un complemento de CNI que proporciona redes de pod.
- Implementación de proveedor de nube: admite la creación de servicios de equilibrador de carga de Kubernetes.

API de Tanzu Kubernetes Grid

Use la API de Tanzu Kubernetes Grid para aprovisionar y administrar clústeres de Tanzu Kubernetes Grid. Se trata de una API declarativa que se invoca mediante kubectl y YAML. Puede descargar el ejecutable de kubectl expandido de VMware desde la dirección IP del endpoint de la API del Supervisor.

Con una API declarativa, en lugar de enviar comandos imperativos al sistema, se especifica el estado deseado del clúster de Tanzu Kubernetes Grid: la cantidad de nodos, el almacenamiento disponible, los tamaños de máquina virtual y la versión de software de Kubernetes. Tanzu Kubernetes Grid se encarga de aprovisionar un clúster que coincide con el estado deseado.

Para llamar a la API de Tanzu Kubernetes Grid, debe invocar kubectl mediante un archivo YAML que, a su vez, invoca la API. Después de crear el clúster, debe actualizar el archivo YAML para actualizar el clúster.

Redes de clústeres de Tanzu Kubernetes Grid

Un clúster de Tanzu Kubernetes Grid que lo aprovisiona Tanzu Kubernetes Grid admite dos opciones de CNI: Antrea (opción predeterminada) y Calico. Ambas opciones son software de código abierto que proporcionan redes para pods, servicios e ingreso del clúster.

Los clústeres de Tanzu Kubernetes Grid aprovisionados por el Tanzu Kubernetes Grid admiten las siguientes opciones de interfaz de red de contenedor (Container Network Interface, CNI):

- Antrea
- Calico

Antrea es el CNI predeterminado para los nuevos clústeres de Tanzu Kubernetes Grid. Si utiliza Antrea, no tiene que especificarlo como CNI durante el aprovisionamiento de los clústeres. Para utilizar Calico como el CNI, tiene dos opciones:

- Especifique el CNI directamente en el YAML del clúster. Consulte Ejemplo de v1alpha3: TKC con red personalizada.
- Cambie el CNI predeterminado. Consulte Ejemplo de v1beta1: clúster con CNI de Calico.

Nota El uso de Antrea como CNI predeterminado requiere una versión mínima del archivo OVA para los clústeres de Tanzu Kubernetes Grid. Consulte Actualizar clústeres de TKG 2 en Supervisor.

En la siguiente tabla se resumen las funciones de redes de los clústeres de Tanzu Kubernetes Grid y su implementación.

Tabla 3-1. Redes de clústeres de Tanzu Kubernetes Grid

Extremo	Proveedor	Descripción
Conectividad de pods	Antrea o Calico	Interfaz de red de contenedor para pods. Antrea utiliza Open vSwitch. Calico utiliza el puente de Linux con BGP.
Tipo de servicio: ClusterIP	Antrea o Calico	Tipo de servicio de Kubernetes predeterminado al que solo se puede acceder en el clúster.
Tipo de servicio: NodePort	Antrea o Calico	Permite el acceso externo a través de un puerto abierto en cada nodo de trabajo mediante el proxy de red de Kubernetes.
Tipo de servicio: LoadBalancer	Equilibrador de carga de NSX-T, NSX Advanced Load Balancer, HAProxy	Para NSX-T, un servidor virtual por definición de tipo de servicio. Para NSX Advanced Load Balancer, consulte esa sección de esta documentación. **Nota** Es posible que algunas características de equilibrio de carga no estén disponibles con HAProxy, como la compatibilidad con IP estáticas.
Entrada de clúster	Controladora de entrada de terceros	Enrutamiento para el tráfico de pods de entrada; puede utilizar cualquier controladora de entrada de terceros, como Contour.
Directiva de red	Antrea o Calico	Controla el tráfico que se permite hacia y desde los pods seleccionados y los endpoints de red. Antrea utiliza Open vSwitch. Calico utiliza tablas de IP de Linux.

Almacenamiento para clústeres de Tanzu Kubernetes Grid

Los clústeres de Tanzu Kubernetes Grid, al igual que otros componentes y cargas de trabajo que se ejecutan en espacios de nombres de Supervisor, requieren almacenamiento persistente.

Directivas de almacenamiento para clústeres de Tanzu Kubernetes Grid

Para proporcionar recursos de almacenamiento persistentes a los clústeres de Tanzu Kubernetes Grid, un administrador de vSphere configura directivas de almacenamiento que describen distintos requisitos de almacenamiento. Después el administrador agrega las directivas de almacenamiento al espacio de nombres en el que se implementa el clúster de Tanzu Kubernetes Grid. Las directivas de almacenamiento visibles para el espacio de nombres determinan a qué almacenes de datos puede acceder al espacio de nombres y cuáles puede utilizar para almacenamiento persistente. Dictan cómo se colocan los nodos del clúster y las cargas de trabajo en el entorno de almacenamiento de vSphere.

Basándose en las directivas de almacenamiento asignadas al espacio de nombres, vSphere IaaS control plane crea clases de almacenamiento de Kubernetes que concuerdan y se muestran automáticamente en el espacio de nombres. También se propagan al clúster de Tanzu Kubernetes Grid en este espacio de nombres.

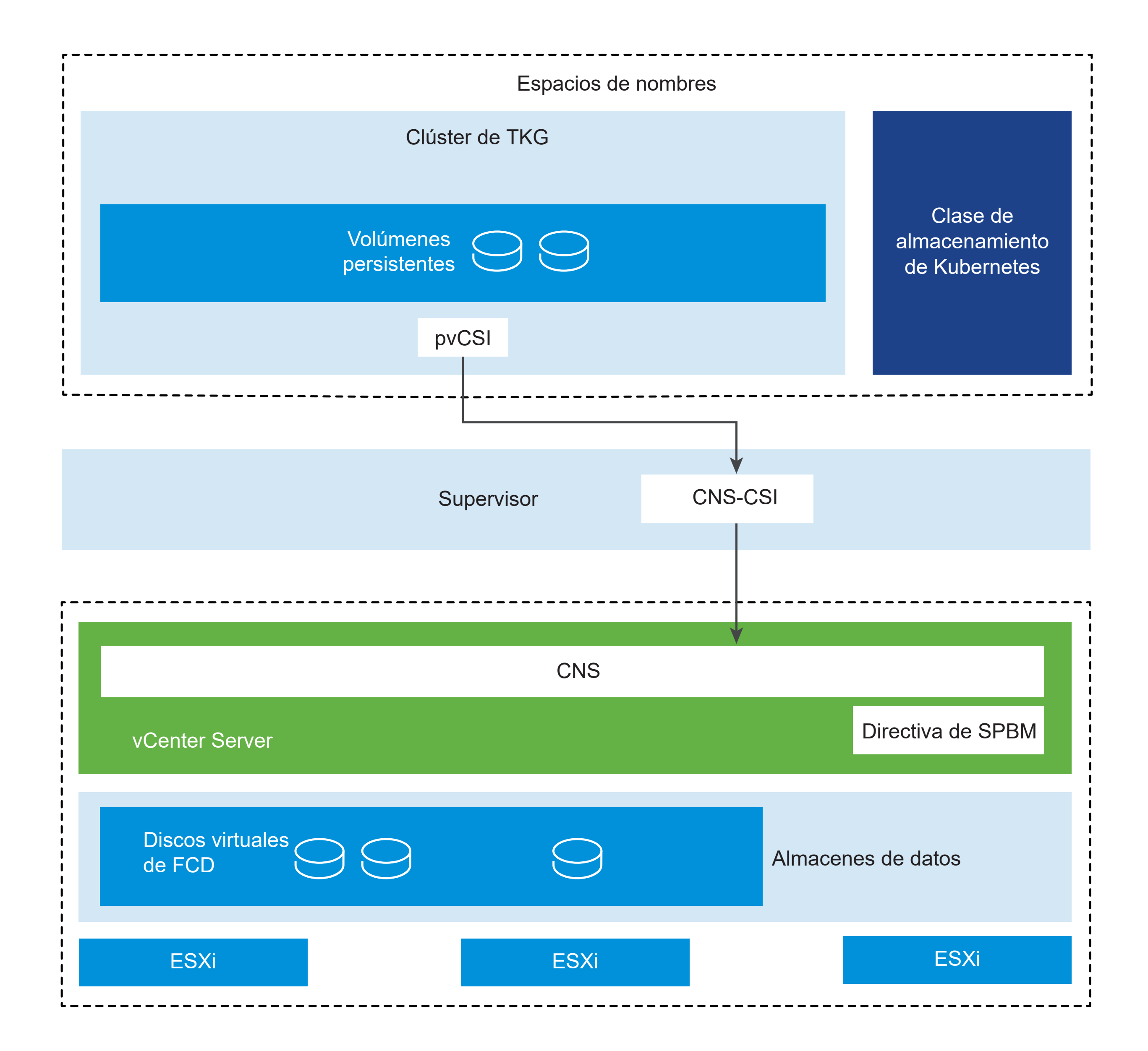
En el clúster de Tanzu Kubernetes Grid, las clases de almacenamiento aparecen en dos ediciones, una con el modo de enlace `Immediate` y otra, con el modo de enlace `WaitForFirstConsumer`. La edición que elija el equipo de desarrollo y operaciones depende de sus requisitos.

Para obtener más información sobre las clases de almacenamiento en clústeres de Tanzu Kubernetes Grid, consulte Usar clases de almacenamiento para volúmenes persistentes.

Cómo se integran los clústeres de Tanzu Kubernetes Grid con el almacenamiento de vSphere

Para integrarse con el Supervisor y el almacenamiento de vSphere, los clústeres de Tanzu Kubernetes Grid usan Paravirtual CSI (pvCSI).

pvCSI es la versión del controlador de CNS-CSI vSphere modificada para los clústeres de Tanzu Kubernetes Grid. pvCSI reside en el clúster de Tanzu Kubernetes Grid y es responsable de todas las solicitudes relacionadas con el almacenamiento que se originan en el clúster de Tanzu Kubernetes Grid. Las solicitudes se envían a CNS-CSI, que a su turno las propaga a CNS en vCenter Server. Como resultado, pvCSI no tiene comunicación directa con el componente de CNS, sino que depende del CNS-CSI para las operaciones de aprovisionamiento de almacenamiento. A diferencia de CNS-CSI, pvCSI no requiere credenciales de infraestructura. Está configurado con una cuenta de servicio en el espacio de nombres.

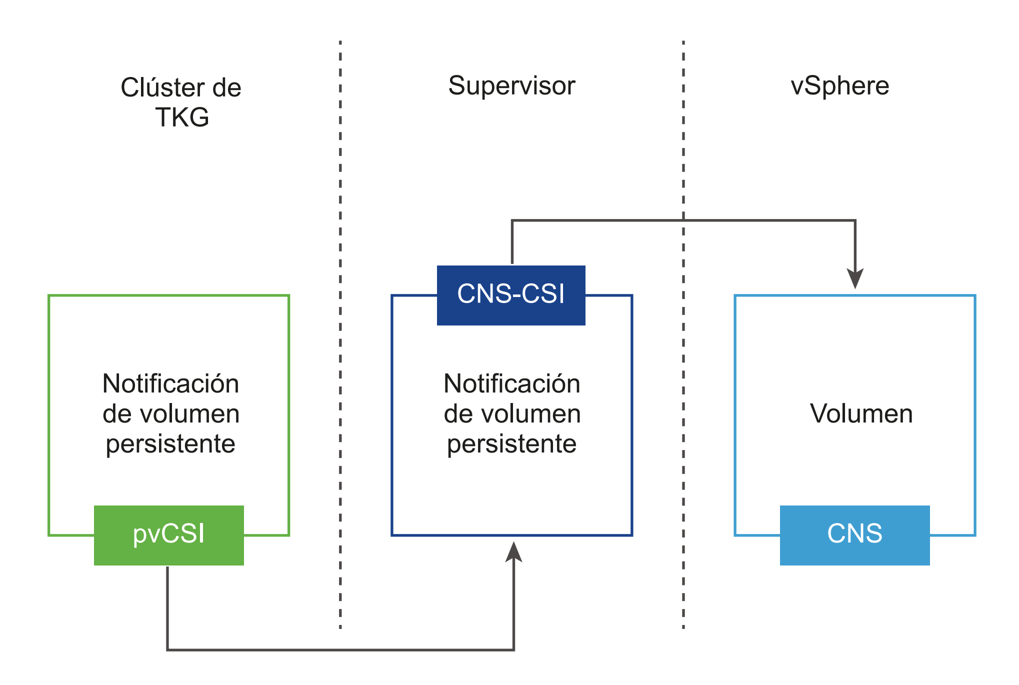


Para obtener información sobre los componentes de Supervisor utilizados para la integración con el almacenamiento de vSphere, consulte Almacenamiento persistente para cargas de trabajo.

Cómo se crea un volumen persistente

A continuación, se muestra cómo interactúan diferentes componentes cuando un ingeniero de desarrollo y operaciones realiza una operación relacionada con el almacenamiento en el clúster de Tanzu Kubernetes Grid, por ejemplo, crea una notificación de volumen persistente (Persistent Volume Claim, PVC).

El ingeniero de desarrollo y operaciones crea un PVC mediante la línea de comandos en el clúster de Tanzu Kubernetes Grid. Esta acción genera una PVC correspondiente en el Supervisor y activa el CNS-CSI. CNS-CSI invoca la API de creación de volumen de CNS.



Después de crear correctamente un volumen, la operación se propaga de vuelta a través del Supervisor al clúster de Tanzu Kubernetes Grid. Como resultado de esta propagación, los usuarios pueden ver el volumen persistente y la notificación de volumen persistente en el estado enlazado en el Supervisor. Además, también verán el volumen persistente y la notificación de volumen persistente en el estado enlazado del clúster de Tanzu Kubernetes Grid.

Funcionalidad admitida por pvCSI

El componente pvCSI que se ejecuta en el clúster de Tanzu Kubernetes Grid admite varias funciones de almacenamiento de vSphere y Kubernetes.

Funcionalidades admitidas	pvCSI con clúster de Tanzu Kubernetes Grid
Compatibilidad de CNS en vSphere Client	Sí
Estado mejorado del objeto en vSphere Client	Sí (solo vSAN)
Volumen persistente de bloques dinámicos (modo de acceso ReadWriteOnce)	Sí
Volumen persistente de archivos dinámicos (modo de acceso ReadWriteMany)	Sí (con Servicios de archivos de vSAN)
Almacén de datos de vSphere	VMFS/NFS/vSAN/vVols
Volumen persistente estático	Sí
Cifrado	No
Expansión de volumen sin conexión	Sí
Expansión de volumen conectado	Sí
Topologías de volumen y zonas	Sí
Varias instancias del plano de control de Kubernetes	Sí
WaitForFirstConsumer	Sí

Funcionalidades admitidas	pvCSI con clúster de Tanzu Kubernetes Grid
VolumeHealth	Sí
Storage vMotion con volúmenes persistentes	No

Alta disponibilidad para clústeres de Tanzu Kubernetes Grid

Puede proporcionar alta disponibilidad a los clústeres de Tanzu Kubernetes Grid cuando están implementados en un Supervisor de tres zonas de vSphere. Una zona de vSphere se asigna a un clúster de vSphere, lo que significa que cuando se implementa un Supervisor en tres zonas de vSphere, utiliza los recursos de los tres clústeres de vSphere subyacentes. Esto protege las cargas de trabajo de Kubernetes que se ejecutan dentro los clústeres de Tanzu Kubernetes Grid contra errores en un nivel de clúster de vSphere. En una implementación de una única zona, vSphere HA proporciona alta disponibilidad para clústeres de Tanzu Kubernetes Grid en un nivel de host ESXi.

En un Supervisor de tres zonas, los nodos del plano de control de los clústeres de Tanzu Kubernetes Grid se colocan automáticamente en las zonas de vSphere. Sin embargo, es posible controlar cómo se distribuyen los nodos de trabajo en las zonas. Puede definir un objeto NodePool para los nodos de trabajo de los clústeres de Tanzu Kubernetes Grid y asignar cada zona de vSphere a un failureDomain dentro de cada NodePool. De esta forma, la API del clúster se encarga de distribuir los nodos de trabajo entre las zonas de vSphere según corresponda. Si omite la especificación de un FailureDomain para uno o todos los NodePools, la API del clúster distribuye automáticamente los NodePools entre las zonas.

Figura 3-2. Alta disponibilidad para clústeres de Tanzu Kubernetes Grid en varias zonas

Autenticación de Tanzu Kubernetes Grid

Aprenda cuáles son los distintos mecanismos de autenticación y su uso con clústeres de Tanzu Kubernetes Grid.

Conexión con el Supervisor

Como ingeniero de desarrollo y operaciones, se conectará al Supervisor para aprovisionar clústeres de Tanzu Kubernetes Grid. Solo tiene acceso a los espacios de nombres a los que el administrador de vSphere le haya concedido permisos.

Para conectarse al Supervisor en la IP del lugar de control de Kubernetes o a clústeres de Tanzu Kubernetes Grid aprovisionados, puede utilizar dos métodos:

- Su vCenter Single Sign-On y las Herramientas de la CLI de Kubernetes para vSphere. En este caso se crea un token de autenticación que caduca cada 10 horas.
- Credenciales de un proveedor de OIDC registrado con el Supervisor y la CLI de Tanzu. La sesión con el proveedor de OIDC se controla mediante la configuración del propio proveedor.

Para obtener más información, consulte la documentación sobre *Uso del servicio TKG con el plano de control de IaaS de vSphere*.

Conectarse a clústeres de Tanzu Kubernetes Grid

Como ingeniero de desarrollo y operaciones, también se conecta a clústeres de Tanzu Kubernetes Grid aprovisionados para operar en ellos y administrarlos. Cuando se concede el permiso Editar a una cuenta de usuario en el espacio de nombres de vSphere en el que se aprovisiona el clúster de Tanzu Kubernetes Grid, a la cuenta se asigna la función `cluster-admin`. Como alternativa, también puede utilizar el usuario `kubernetes-admin` para conectarse a los clústeres de Tanzu Kubernetes Grid. También puede conceder a los desarrolladores acceso a los clústeres de Tanzu Kubernetes Grid enlazando un usuario o grupo a la directiva de seguridad de pods predeterminada o personalizada. Para obtener más información, consulte la documentación sobre *Uso del servicio TKG con el plano de control de IaaS de vSphere*.

Opciones de implementación de Supervisor

4

Comprobar cuáles son las opciones para implementar y configurar un Supervisor. Según la pila de redes o la opción de implementación que implemente para el Supervisor, las topologías admitidas y los tipos de carga de trabajo admitidos son diferentes.

Lea los siguientes temas a continuación:

Implementaciones de clúster y de Supervisor zonal

Conozca cuáles son las diferencias entre implementar un Supervisor en tres clústeres de vSphere asignados a zonas de vSphere y una implementación en un solo clúster del Supervisor que se asigna a una zona de vSphere.

Nota Una vez que implemente una instancia de Supervisor en un clúster de vSphere único, lo que provocará la creación de una zona de vSphere, no podrá expandir Supervisor a una implementación de tres zonas. Puede implementar una instancia de Supervisor en una zona de vSphere (implementación de un solo clúster) o en tres zonas de vSphere.

Implementación en tres zonas del Supervisor para HA en el nivel de clúster

Puede habilitar vSphere IaaS control plane en tres clústeres de vSphere que están asignados a tres zonas de vSphere. Configure cada clúster de vSphere como un dominio de errores independiente y asígnelo a una zona de vSphere. En una implementación de tres zonas, los tres clústeres de vSphere se convierten en un Supervisor. En una implementación de tres zonas, puede:

- Proporcionar alta disponibilidad en el nivel de clúster al Supervisor, ya que cada clúster de vSphere es un dominio de errores independiente.

- Distribuir los nodos de sus clústeres de Tanzu Kubernetes Grid en las tres zonas de vSphere de modo que proporcione HA a sus cargas de trabajo de Kubernetes en un nivel de clúster de vSphere.
- Escalar el Supervisor agregando hosts a cada uno de los tres clústeres de vSphere.

Puede ejecutar cargas de trabajo en una instancia de Supervisor de tres zonas mediante el uso de clústeres de Tanzu Kubernetes Grid, pods de vSphere y máquinas virtuales.

Figura 4-1. Implementación de Supervisor de tres zonas

vCenter Server
Clústeres de Tanzu Kubernetes Grid
Máquinas virtuales
Espacio de nombres de vSphere
Supervisor
Zona A
Máquina virtual de plano de control 1
Clúster de vSphere 1
Zona B
Máquina virtual de plano de control 1
Clúster de vSphere 2
Zona C
Máquina virtual de plano de control 1
Clúster de vSphere 3

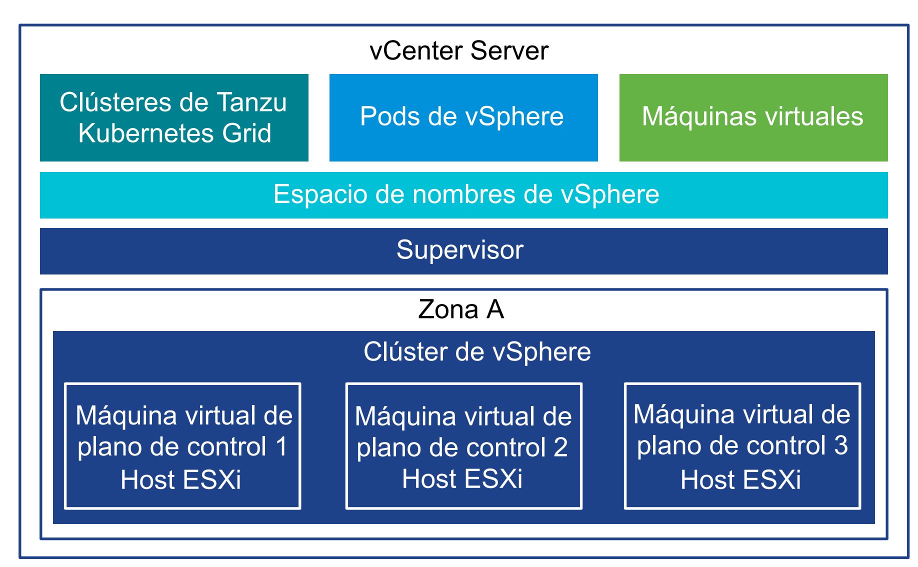
Colocación de zonas de vSphere en sitios físicos

Puede distribuir las zonas de vSphere entre diferentes sitios físicos siempre que la latencia entre los sitios no supere los 100 ms. Por ejemplo, puede distribuir las zonas de vSphere entre dos sitios físicos: una zona de vSphere en el primer sitio y dos en el segundo sitio.

Implementación de clúster único del Supervisor

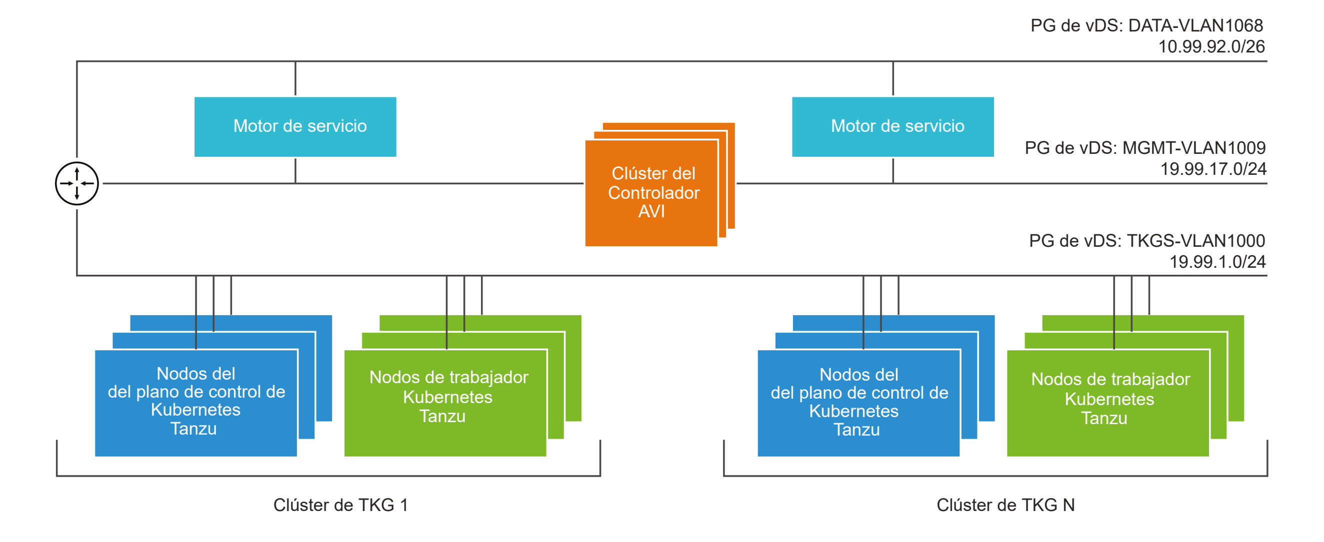
Aún puede habilitar un Supervisor en un clúster único de vSphere. En este caso, se crea automáticamente una zona para el Supervisor, o bien, puede utilizarse una zona que se haya creado de antemano. En una implementación en un solo clúster, seguirá teniendo alta disponibilidad en el nivel de clúster a través de vSphere HA, y solo puede escalar la configuración de vSphere IaaS control plane agregando hosts al clúster de vSphere que se asigna a Supervisor. En una implementación de clúster único, puede ejecutar cargas de trabajo a través de pods de vSphere, clústeres de Tanzu Kubernetes Grid y máquinas virtuales implementadas a través del servicio de máquina virtual.

Figura 4-2. Implementación de Supervisor de un clúster



Topología para Supervisor con redes VDS y NSX Advanced Load Balancer

El controlador AVI siempre se implementa en la red de administración, donde puede establecer una interfaz con vCenter Server, los hosts ESXi y los nodos del plano de control del Supervisor. Los motores de servicio se implementan con interfaces en la red de administración y la red de datos.



La red de administración, como `MGMT-VLAN1009`, es donde se encuentra el controlador y donde se conecta la interfaz de administración de los motores de servicios.

La red de datos, como `DATA-VLAN1068`, es donde se conectan las interfaces del motor de servicio para la colocación de VIP. El tráfico del cliente llega a la VIP y los motores de servicio equilibran la carga del tráfico a las direcciones IP de la red de cargas de trabajo a través de esta red.

La red de cargas de trabajo, como `TKGS-VLAN1000`, es donde se ejecutan los clústeres de Tanzu Kubernetes Grid. Los motores de servicio no requieren interfaces con la red de cargas de trabajo.

Los motores de servicio se ejecutan en modo one-arm. Enrutan el tráfico con equilibrio de carga a la red de cargas de trabajo a través del enrutador. Los motores de servicio no obtienen la IP de puerta de enlace predeterminada de DHCP en las redes de datos. Debe configurar rutas estáticas para que los motores de servicio puedan enrutar el tráfico a las redes de carga de trabajo y la IP del cliente correctamente.

Esta topología permite que el motor de servicio se encuentre en una única red. El controlador AVI automatiza la creación del motor de servicio y las conexiones de red.

Para obtener información sobre cómo instalar y configurar NSX Advanced Load Balancer, consulte Instalar y configurar NSX Advanced Load Balancer.

Componentes de NSX Advanced Load Balancer

Los componentes de NSX Advanced Load Balancer, también conocido como Equilibrador de carga de AVI, incluyen el clúster del controlador, las máquinas virtuales de los motores de servicio (plano de datos) y el operador de AVI Kubernetes (AKO).

Para obtener información sobre cómo instalar y configurar los componentes de NSX Advanced Load Balancer, consulte Instalar y configurar NSX Advanced Load Balancer.

Controladora

El controlador de NSX Advanced Load Balancer, también conocido como el Controlador, interactúa con vCenter Server para automatizar el equilibrio de carga de los clústeres de Tanzu Kubernetes Grid. Se encarga de aprovisionar los motores de servicio, coordinar los recursos entre los motores de servicio y agregar métricas y registros de los motores de servicio. El controlador proporciona una interfaz web, una interfaz de línea de comandos y una API para la operación del usuario y la integración programática.

Después de implementar y configurar la máquina virtual del controlador en vSphere, consulte si puede implementar un clúster de controladores para configurar el clúster del plano de control para HA.

Las nubes son contenedores del entorno en el que está instalado o funciona NSX Advanced Load Balancer. Durante la configuración inicial del controlador, se crea automáticamente una nube con el nombre **Nube predeterminada**. Puede utilizar la **Nube predeterminada** como una nube de **VMware vCenter** o crear una o varias nubes personalizadas del tipo **VMware vCenter**.

Al configurar un tipo de nube de **VMware vCenter**, este se asocia con un vCenter único y un centro de datos dentro de ese vCenter. Todos los recursos que están disponibles para ese vCenter y el centro de datos están disponibles para la nube.

Para permitir que el equilibrador de carga pueda atender varias instancias de vCenter Server o varios centros de datos, puede crear varias nubes personalizadas del tipo **VMware vCenter**, una para cada combinación de vCenter y centro de datos. Esto reduce la carga de operaciones, ya que se requieren menos instancias del equilibradores de carga y, por lo tanto, menos núcleos para respaldar el entorno. Para obtener más información sobre las nubes, consulte la documentación de NSX Advanced Load Balancer.

Motor de servicio

El motor de servicio de NSX Advanced Load Balancer, también conocido como motor de servicio, es la máquina virtual del plano de datos. Un motor de servicio ejecuta uno o varios servicios virtuales. El controlador administra un motor de servicio. El controlador aprovisiona los motores de servicio para alojar servicios virtuales.

El motor de servicio tiene dos tipos de interfaces de red:

- La primera interfaz de red, `vnic0` de la máquina virtual, se conecta a la red de administración, donde puede conectarse al controlador de NSX Advanced Load Balancer.
- Las restantes interfaces, `vnic1 - 9`, se conectan a la red de datos en la que se ejecutan los servicios virtuales.

Las interfaces del motor de servicio se conectan automáticamente a los grupos de puertos de vDS correctos. Las interfaces sin utilizar se conectan a un grupo de puertos de la red de administración en un estado desconectado. Cada motor de servicio puede admitir hasta 1000 servicios virtuales.

Un servicio virtual proporciona servicios de equilibrio de carga de capa 4 y capa 7 para cargas de trabajo del clúster de Tanzu Kubernetes Grid. Un servicio virtual se configura con una IP virtual y varios puertos. Cuando se implementa un servicio virtual, el controlador selecciona automáticamente una instancia de ESX Server, aumenta la velocidad de giro de un motor de servicio y lo conecta a las redes correctas (grupos de puertos).

El primer motor de servicio solo se crea después de configurar el primer servicio virtual. Todos los servicios virtuales que se configuren posteriormente utilizarán el motor de servicio existente.

Cada servidor virtual expone un equilibrador de carga de capa 4 con una dirección IP distinta del tipo equilibrador de carga para un clúster de Tanzu Kubernetes Grid. La dirección IP asignada a cada servidor virtual se selecciona en el bloque de direcciones IP otorgado al controlador cuando se configura.

AVI es compatible con proveedores de IPAM nativo e IPAM externo. En vSphere, se aprovecha el IPAM nativo de AVI.

Operador de AVI Kubernetes

El operador de AVI Kubernetes (AKO) consulta los recursos de Kubernetes y se comunica con el controlador para solicitar los recursos de equilibrio de carga correspondientes.

El operador de AVI Kubernetes se instala en los Supervisores como parte del proceso de habilitación.

Topologías para un Supervisor de una zona con NSX como pila de redes

vSphere IaaS control plane se puede implementar en dos clústeres, uno para las funciones de Edge y de administración, y otro dedicado a la administración de cargas de trabajo.

Figura 4-3. Clústeres de administración de cargas de trabajo, Edge y administración

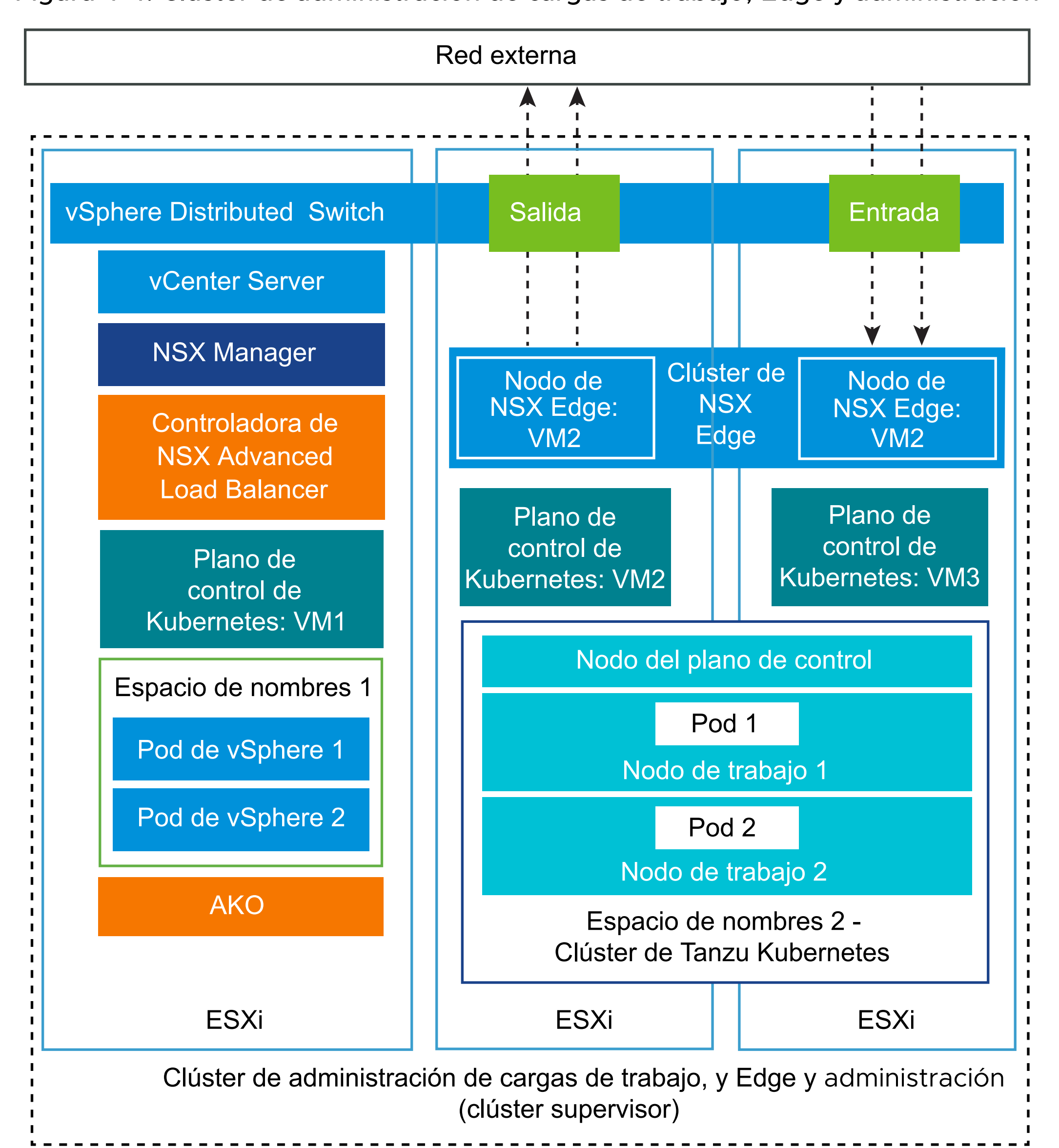
Topologías para un Supervisor de una zona con NSX como pila de redes y NSX Advanced Load Balancer

Puede aplicar diferentes topologías al Supervisor dependiendo de las necesidades de sus cargas de trabajo de Kubernetes y de la infraestructura de redes subyacente.

Topología para un clúster de dominio de carga de trabajo, Edge y administración

vSphere IaaS control plane se puede implementar con funciones de administración de cargas de trabajo, Edge y administración combinada en un único clúster de vSphere.

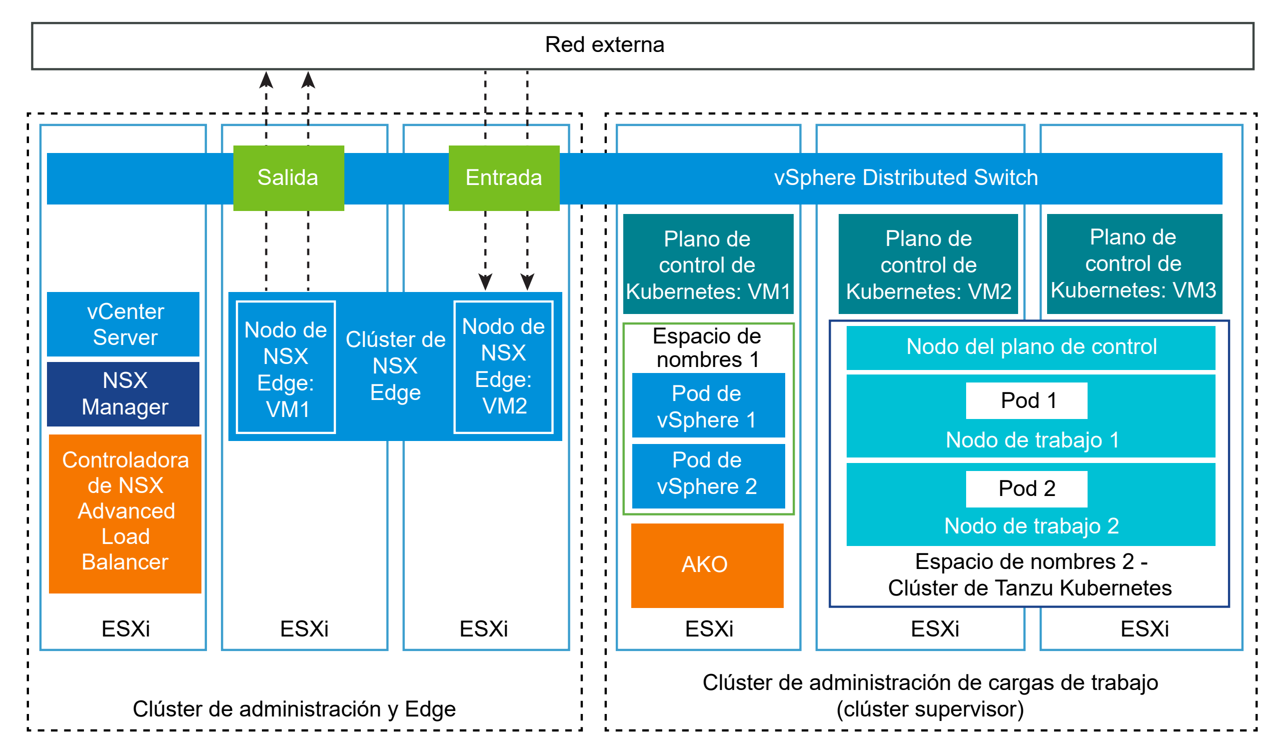
Figura 4-4. Clúster de administración de cargas de trabajo, Edge y administración



Topología con clúster de administración y Edge y clúster de administración de cargas de trabajo independientes

vSphere IaaS control plane se puede implementar en dos clústeres, uno para las funciones de Edge y de administración, y otro dedicado a la administración de cargas de trabajo.

Figura 4-5. Clústeres de administración de cargas de trabajo, Edge y administración



Topologías para implementar el equilibrador de carga de HAProxy

Revise las posibles topologías que puede implementar para el equilibrador de carga de HAProxy para un Supervisor configurado con redes VDS. Al usar vSphere IaaS control plane con redes VDS, HAProxy brinda equilibrio de carga para desarrolladores que acceden al plano de control de Tanzu Kubernetes Grid y para los servicios de Kubernetes del tipo equilibrador de carga.

Redes de carga de trabajo en el Supervisor

Para configurar una instancia de Supervisor con redes VDS, debe conectar todos los hosts del clúster a una instancia de VDS. En función de la topología que implemente para las redes de carga de trabajo de Supervisor, cree uno o varios grupos de puertos distribuidos. Los grupos de puertos se designan como redes de cargas de trabajo para los espacios de nombres de vSphere.

Las redes de cargas de trabajo proporcionan conectividad a los nodos de los clústeres de Tanzu Kubernetes Grid y a las máquinas virtuales del plano de control de Supervisor. La red de cargas de trabajo que proporciona conectividad a las máquinas virtuales del plano de control de Kubernetes se denomina red de carga de trabajo principal. Cada Supervisor debe tener una red de cargas de trabajo principal. Debe designar uno de los grupos de puertos distribuidos como la red de cargas de trabajo principal para Supervisor.

Nota Las redes de carga de trabajo solo se agregan cuando habilita el Supervisor y no se pueden agregar más adelante.

Las máquinas virtuales del plano de control de Kubernetes en Supervisor usan tres direcciones IP del rango de direcciones IP que se asigna a la red de cargas de trabajo principal. Cada nodo de un clúster de Tanzu Kubernetes Grid tiene una dirección IP independiente asignada desde el rango de direcciones de la red de cargas de trabajo que está configurada con el espacio de nombres en el que se ejecuta el clúster de Tanzu Kubernetes Grid.

Asignación de rangos de direcciones IP

Cuando planifique la topología de red de Supervisor con el equilibrador de carga de HA Proxy, planee tener dos tipos de rangos de direcciones IP:

- Un rango para asignar direcciones IP virtuales para HAProxy. El rango de IP que se configura para los servidores virtuales de HAProxy está reservado por el dispositivo del equilibrador de carga. Por ejemplo, si el rango de direcciones IP virtuales es `192.168.1.0/24`, no se podría acceder a todos los hosts de ese rango para otro tráfico que no sea el tráfico de IP virtual.

  Nota No debe configurar una puerta de enlace dentro del rango de direcciones IP virtuales de HAProxy, ya que se podrían generar errores en todas las rutas a esa puerta de enlace.

- Un rango de direcciones IP para los nodos de Supervisor y los clústeres de Tanzu Kubernetes Grid. Cada máquina virtual del plano de control de Kubernetes en Supervisor tiene asignada una dirección IP, lo que supone un total de tres direcciones IP. Cada nodo de un clúster de Tanzu Kubernetes Grid también tiene asignada una dirección IP independiente. Debe asignar un rango de direcciones IP único a cada red de cargas de trabajo en el Supervisor que configure en un espacio de nombres.

Ejemplo de una configuración con una red de /24:

- Red: 192.168.120.0/24
- VIP de HAProxy: 192.168.120.128/25
- 1 dirección IP para la interfaz de carga de trabajo de HAProxy: 192.168.120.5

En función de las direcciones IP que estén libres en las primeras 128 direcciones, puede definir rangos de IP para las redes de cargas de trabajo en Supervisor, por ejemplo:

- 192.168.120.31-192.168.120.40 para la red de cargas de trabajo principal
- 192.168.120.51-192.168.120.60 para otra red de cargas de trabajo

Nota Los rangos que defina para las redes de cargas de trabajo no deben superponerse con el rango de VIP de HAProxy.

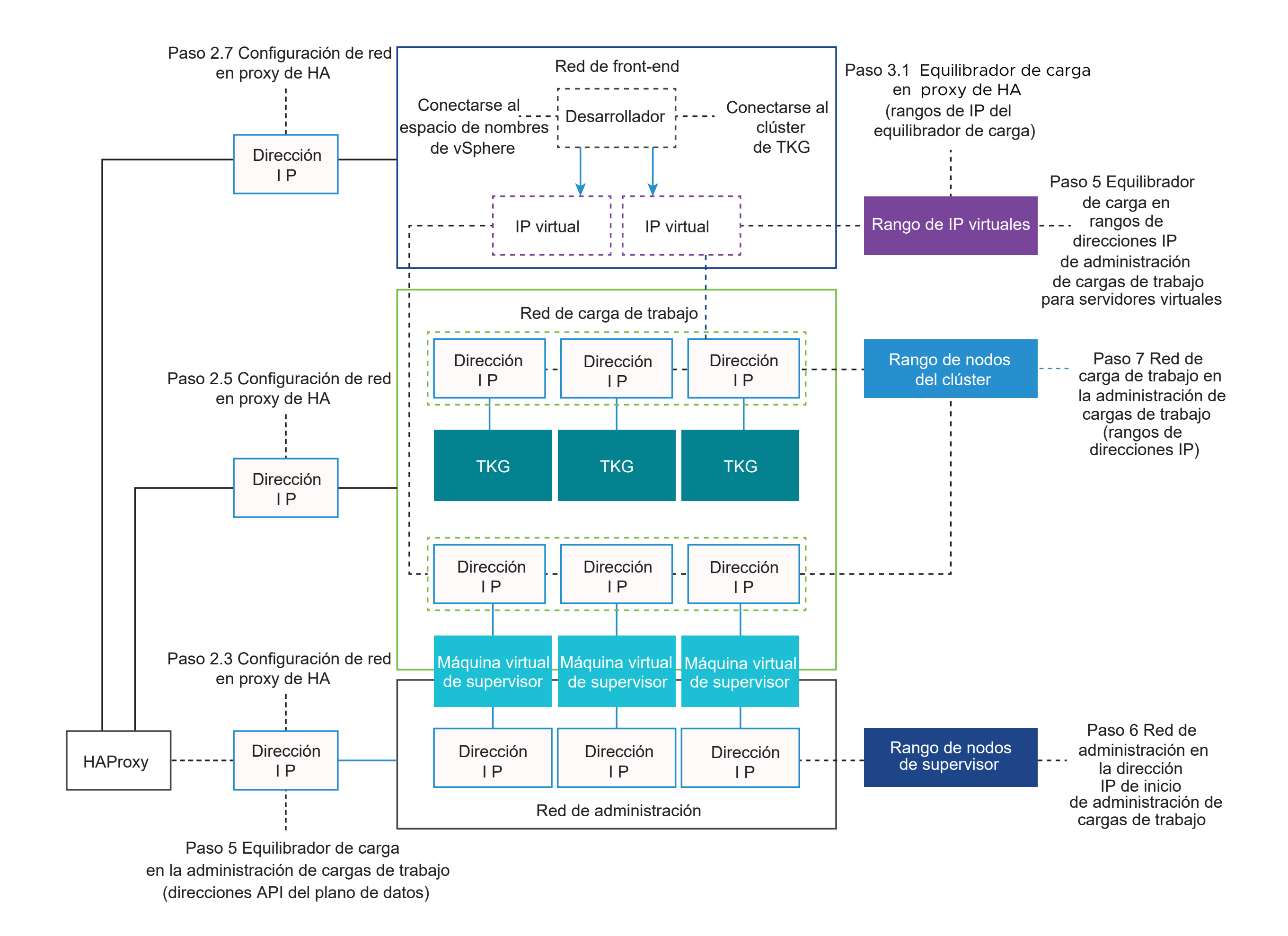
Topología de red de HAProxy

Existen dos opciones de configuración de red para implementar HAProxy: **Predeterminada** y **Front-end**. La red predeterminada tiene 2 NIC: una para la red de administración y otra para la red de cargas de trabajo. La red de front-end tiene 3 NIC: red de administración, red de cargas de trabajo y red de front-end para los clientes. En la tabla se enumeran y describen las características de cada red.

En el caso de las instalaciones de producción, se recomienda implementar el equilibrador de carga de HAProxy con la configuración de **Red de front-end**. Si implementa el equilibrador de carga de HAProxy con la configuración **Predeterminada**, se recomienda asignar un tamaño de bloque de direcciones IP de /24 a la red de cargas de trabajo. Para ambas opciones de configuración, no se recomienda utilizar DHCP.

Red	Características
Administración	El clúster supervisor utiliza la red de administración para conectarse al equilibrador de carga de HAProxy y programarlo. ■ El endpoint de la API del plano de datos de HAProxy está enlazado a la interfaz de red conectada a la red de administración. ■ La dirección IP de administración asignada a la máquina virtual del plano de control de HAProxy debe ser una dirección IP estática en la red de administración, de modo que el clúster supervisor pueda conectarse con confianza a la API del equilibrador de carga. ■ La puerta de enlace predeterminada de la máquina virtual de HAProxy debe estar en esta red. ■ Las consultas de DNS deben realizarse en esta red.
Carga de trabajo	La máquina virtual del plano de control de HAProxy utiliza la red de cargas de trabajo para acceder a los servicios de los nodos del clúster supervisor y del clúster de Tanzu Kubernetes. ■ La máquina virtual del plano de control de HAProxy reenvía el tráfico a los nodos del clúster supervisor y del clúster de Tanzu Kubernetes en esta red. ■ Si la máquina virtual del plano de control de HAProxy se implementa en el modo predeterminado (dos NIC), la red de cargas de trabajo debe proporcionar las redes lógicas que se utilizarán para acceder a los servicios del equilibrador de carga. ■ En la configuración **Predeterminada**, las direcciones IP virtuales del equilibrador de carga y las direcciones IP del nodo del clúster de Kubernetes proceden de esta red. Se definirán como rangos independientes que no se superponen dentro de la red. **Nota** La red de carga de trabajo debe estar en una subred diferente a la red de administración. Consulte los Requisitos para la implementación de clústeres de Supervisor con redes VDS y equilibrador de carga de HAProxy.
Front-end (opcional)	Los clientes externos (como usuarios o aplicaciones) que acceden a las cargas de trabajo del clúster usan la red de front-end para acceder a los servicios con carga equilibrada del back-end mediante direcciones IP virtuales. ■ La red de front-end solo se utiliza cuando la máquina virtual del plano de control de HAProxy se implementa con tres NIC. ■ Esta opción se recomienda para instalaciones de producción. ■ La red de front-end es donde muestra la dirección IP virtual (VIP). HAProxy equilibrará y reenviará el tráfico al back-end adecuado.

En el siguiente diagrama se muestra una implementación de HAProxy con una topología de **red de front-end**. El diagrama indica dónde se espera que estén los campos de configuración durante el proceso de instalación y configuración.



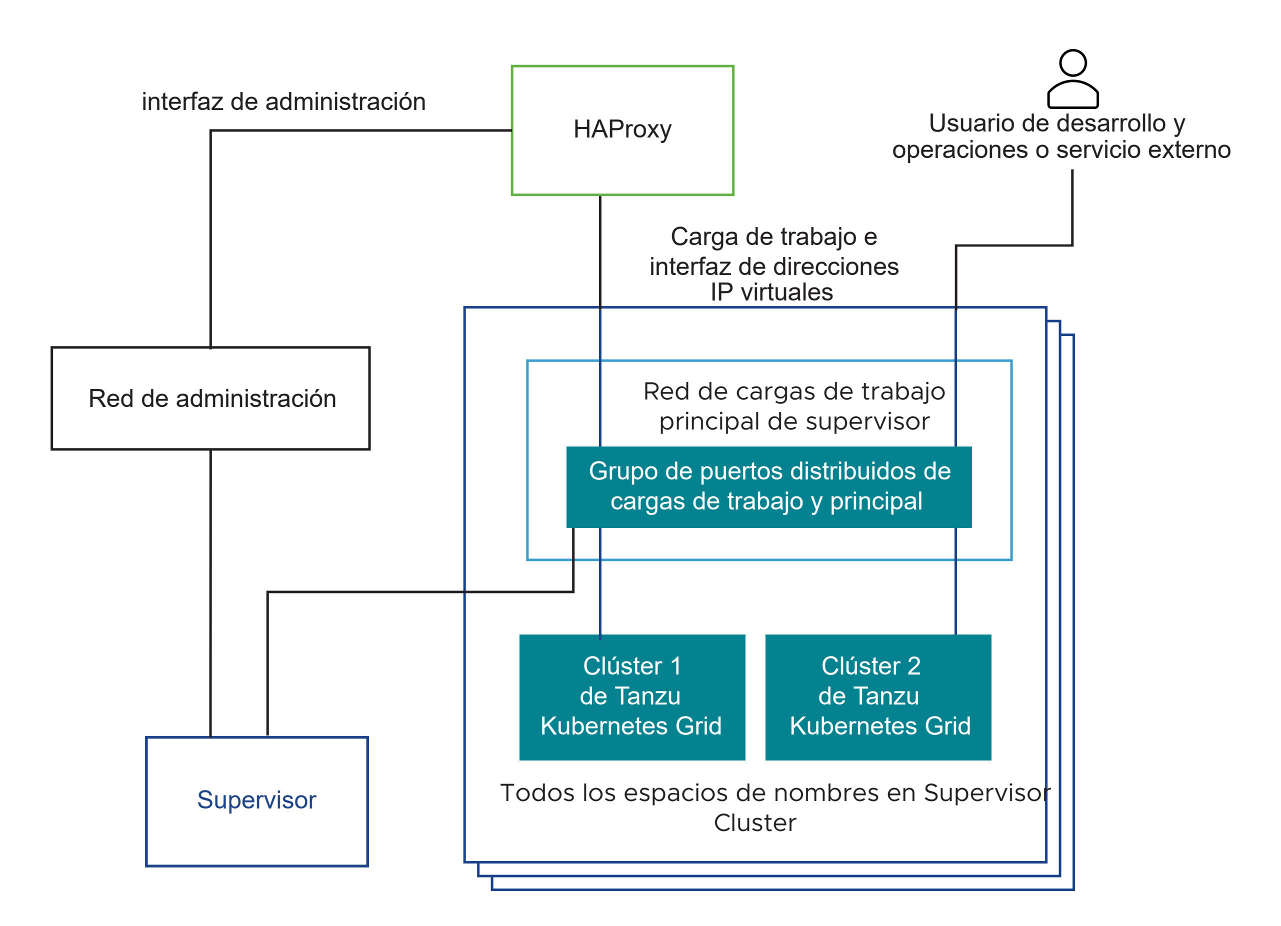
Topología de Supervisor con una red de cargas de trabajo y HAProxy con dos NIC virtuales

En esta topología, se configura un Supervisor con una red de carga de trabajo para los siguientes componentes:

- Máquinas virtuales de plano de control de Kubernetes
- Los nodos de los clústeres de Tanzu Kubernetes Grid.
- El rango de IP virtuales de HAProxy donde se conectan los servicios externos y los usuarios de desarrollo y operaciones. En esta configuración, HAProxy se implementa con dos NIC virtuales (configuración **Predeterminada**), una conectada a la red de administración y otra conectada a la red de cargas de trabajo principal. Debe planificar la asignación de direcciones IP virtuales en una subred independiente de la red de cargas de trabajo principal.

Designe un grupo de puertos como red de cargas de trabajo principal para el Supervisor y, a continuación, utilice el mismo grupo de puertos como red de cargas de trabajo para los espacios de nombres de vSphere. El Supervisor, los clústeres de Tanzu Kubernetes Grid, HAProxy, los usuarios de desarrollo y operaciones y los servicios externos se conectan al mismo grupo de puertos distribuidos que se establece como red de cargas de trabajo principal.

Figura 4-6. Supervisor respaldado por una red



La ruta de tráfico para los usuarios de desarrollo y operaciones o las aplicaciones externas es la siguiente:

1 El usuario de desarrollo y operaciones o el servicio externo envían tráfico a una dirección IP virtual en la subred de red de cargas de trabajo del grupo de puertos distribuidos.

2 La carga de HAProxy equilibra el tráfico de IP virtual con la dirección IP del nodo del clúster de Tanzu Kubernetes Grid o con la dirección IP de la máquina virtual del plano de control. HAProxy reclama la dirección IP virtual para que pueda equilibrar la carga del tráfico que entra en esa IP.

3 La máquina virtual del plano de control o el nodo del clúster de Tanzu Kubernetes Grid entrega el tráfico a los pods de destino que se ejecutan dentro del Supervisor o el clúster de Tanzu Kubernetes Grid, respectivamente.

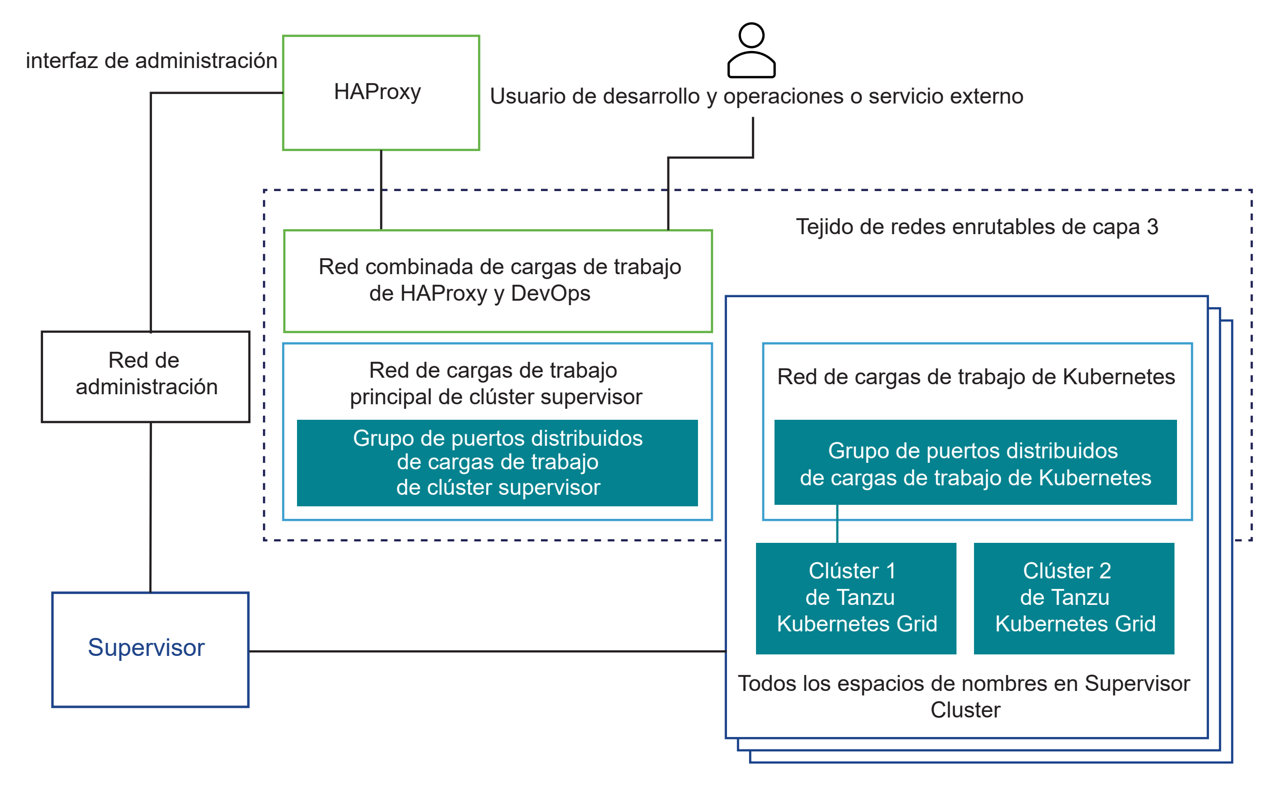
Topología de Supervisor con una red de carga de trabajo aislada y HA Proxy con dos NIC virtuales

En esta topología, se configuran redes para los siguientes componentes:

- Máquinas virtuales del plano de control de Kubernetes. Una red de cargas de trabajo principal para controlar el tráfico de las máquinas virtuales del plano de control de Kubernetes.
- Nodos del clúster de Tanzu Kubernetes Grid. Una red de cargas de trabajo. que asigna a todos los espacios de nombres del Supervisor. Esta red conecta los nodos del clúster de Tanzu Kubernetes Grid.
- IP virtuales de HAProxy. En esta configuración, la máquina virtual de HAProxy se implementa con dos NIC virtuales (configuración **Predeterminada**). Puede conectar la máquina virtual de HAProxy a la red de cargas de trabajo principal o a la red de cargas de trabajo que utiliza para los espacios de nombres. También puede conectar HAProxy a una red de máquinas virtuales que ya exista en vSphere y que se pueda enrutar a las redes principal y de cargas de trabajo.

El Supervisor está conectado al grupo de puertos distribuidos que respalda la red de cargas de trabajo principal y los clústeres de Tanzu Kubernetes Grid están conectados a un grupo de puertos distribuidos que respalda la red de cargas de trabajo. Los dos grupos de puertos deben ser enrutables de capa 3. El aislamiento de la capa 2 se puede implementar a través de las VLAN. El filtrado de tráfico de la capa 3 es posible a través de las puertas de enlace y los firewalls de IP.

Figura 4-7. Supervisor con una red de cargas de trabajo aislada



La ruta de tráfico para el servicio externo o los usuarios de desarrollo y operaciones es la siguiente:

1 El servicio externo o el usuario de desarrollo y operaciones envía tráfico a una dirección IP virtual. El tráfico se enruta a la red donde se conecta HAProxy.

2 HAProxy equilibra la carga del tráfico de IP virtual con la dirección IP del nodo de Tanzu Kubernetes Grid o la máquina virtual del plano de control. HAProxy reclama la dirección IP virtual para que pueda equilibrar la carga del tráfico que entra en esa IP.

3 La máquina virtual del plano de control o el nodo del clúster de Tanzu Kubernetes Grid entrega el tráfico a los pods de destino que se ejecutan dentro del clúster de Tanzu Kubernetes Grid.

Topología de Supervisor con una red de carga de trabajo múltiple y HA Proxy con dos NIC virtuales

En esta topología, es posible configurar un grupo de puertos para que actúe como red de cargas de trabajo principal y un grupo de puertos dedicados que sirvan como red de cargas de trabajo para cada espacio de nombres. HAProxy se implementa con dos NIC virtuales (configuración **Predeterminada**) y puede conectarse a la red de cargas de trabajo principal o a cualquiera de las redes de cargas de trabajo. También puede utilizar una red de máquinas virtuales existente que se pueda enrutar a las redes principal y de cargas de trabajo.

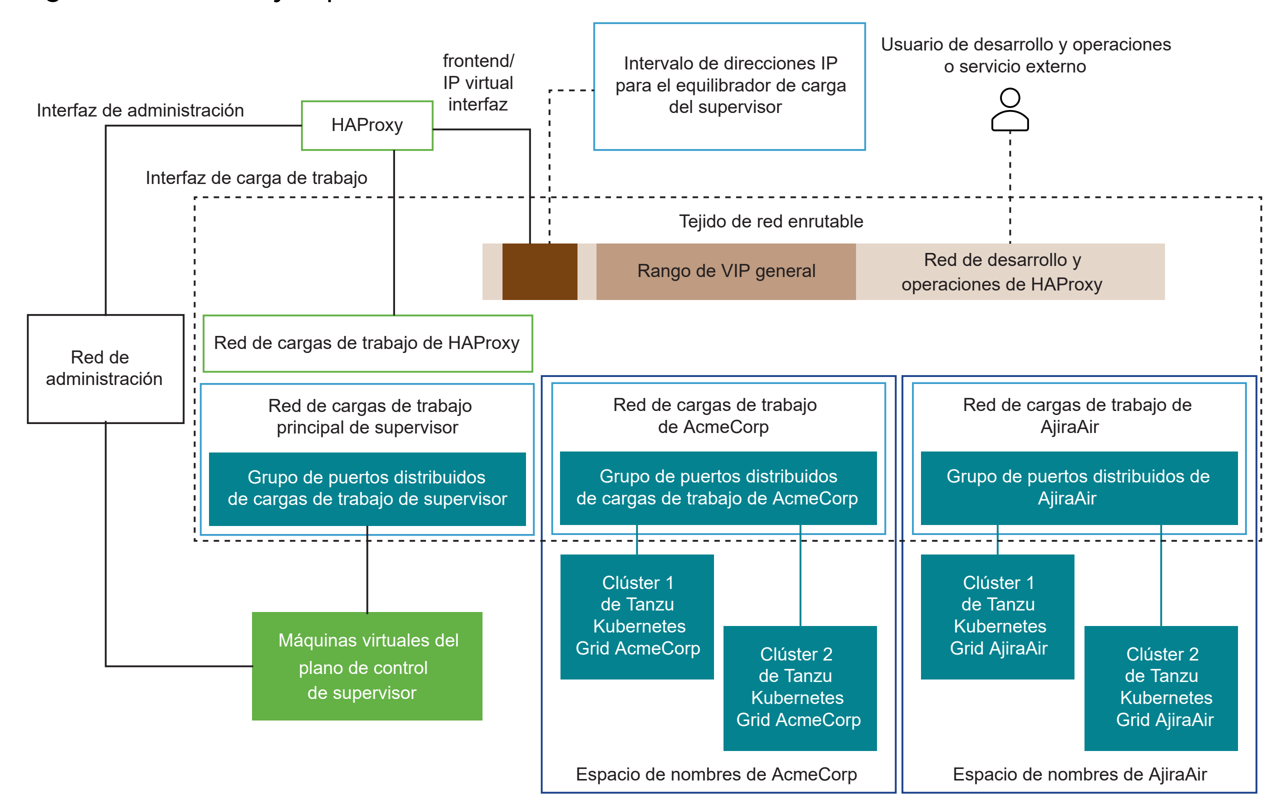
La ruta de tráfico para los servicios externos o los usuarios de desarrollo y operaciones en esta topología es la misma que la de la topología de red de cargas de trabajo aislada.

Figura 4-8. Instancia de Supervisor respaldada por varias redes de cargas de trabajo aisladas

Topología de Supervisor con una red de carga de trabajo múltiple y HA Proxy con tres NIC virtuales

En esta configuración, se implementa la máquina virtual de HAProxy con tres NIC virtuales, por lo que HAProxy se conecta a una red de front-end. Los usuarios y los servicios externos de desarrollo y operaciones pueden acceder a HAProxy a través de IPs virtuales en la red front-end. Se recomienda implementar HA Proxy con tres NIC virtuales para entornos de producción.

Figura 4-9. HAProxy implementado con tres NIC virtuales



Seleccionar entre las posibles topologías

Antes de seleccionar alguna de las posibles topologías, debe evaluar las necesidades de su entorno:

1 ¿Necesita el aislamiento de Capa 2 entre el Supervisor y los clústeres de Tanzu Kubernetes Grid?

   a No: la topología más simple, con una red de cargas de trabajo que atienda a todos los componentes.

   b Sí: la topología de red de cargas de trabajo aislada con redes principal y de cargas de trabajo independientes.

2 ¿Necesita aún más aislamiento de Capa 2 entre los clústeres de Tanzu Kubernetes Grid?

   a No: topología de red de cargas de trabajo aislada con redes principal y de cargas de trabajo independientes.

b Sí: topología con varias redes de cargas de trabajo con una red de cargas de trabajo independiente para cada espacio de nombres y una red de cargas de trabajo principal dedicada.

3 ¿Desea evitar que los usuarios de desarrollo y operaciones y los servicios externos enruten directamente a las máquinas virtuales del plano de control de Kubernetes y los nodos del clúster de Tanzu Kubernetes Grid?

   a No: configuración de HAProxy con dos NIC.

   b Sí: configuración de HAProxy con tres NIC Esta configuración se recomienda para entornos de producción.

Consideraciones sobre el uso del equilibrador de carga de HAProxy con vSphere IaaS control plane

Tenga en cuenta las siguientes consideraciones al planificar una instancia de vSphere IaaS control plane con el equilibrador de carga de HAProxy.

- Se requiere un contrato de soporte con HAProxy para obtener soporte técnico para el equilibrador de carga de HAProxy. VMware GSS no puede proporcionar compatibilidad con el dispositivo de HAProxy .
- El dispositivo de HAProxy es un singleton sin posibilidad de disponer de una topología de alta disponibilidad. Para entornos de alta disponibilidad, VMware recomienda utilizar una instalación completa de NSX o NSX Advanced Load Balancer.
- No es posible expandir el rango de direcciones IP utilizado para el front-end en una fecha posterior, lo que significa que la red debe dimensionarse para todo el crecimiento futuro.

Requisitos para la implementación de Supervisor zonal

5

Revise los requisitos para habilitar un Supervisor en las zonas de vSphere. Las zonas de vSphere habilitadas para Supervisor proporcionan alta disponibilidad a las cargas de trabajo de Kubernetes en un nivel de clúster de vSphere.

Nota Si actualizó el entorno de vSphere IaaS control plane de una versión de vSphere anterior a la 8.0 y desea utilizar zonas de vSphere para las implementaciones, como los clústeres de Tanzu Kubernetes Grid, debe crear un nuevo Supervisor de tres zonas. vSphere IaaS control plane no admite la conversión del Supervisor desde un solo clúster a uno de tres zonas.

Lea los siguientes temas a continuación:

- Requisitos para la implementación de Supervisor zonal con redes VDS y NSX Advanced Load Balancer
- Requisitos para Supervisor zonal con NSX
- Requisitos para Supervisor zonal con NSX y NSX Advanced Load Balancer
- Requisitos para la implementación de un Supervisor zonal con equilibrador de carga de HAProxy

Requisitos para la implementación de Supervisor zonal con redes VDS y NSX Advanced Load Balancer

Consulte los requisitos para habilitar una instancia de Supervisor con redes VDS y NSX Advanced Load Balancer en tres clústeres de vSphere asignados a tres zonas de vSphere. Para configurar vSphere IaaS control plane con el NSX Advanced Load Balancer, también conocido como equilibrador de carga de AVI, el entorno debe cumplir ciertos requisitos. vSphere IaaS control plane admite varias topologías: una única red de vDS para los servicios del motor de servicio de AVI y del equilibrador de carga, y un vDS para el plano de administración de AVI y otro VDS para el NSX Advanced Load Balancer.

Redes de cargas de trabajo

Para configurar una instancia de Supervisor con la pila de redes VDS, debe conectar todos los hosts del clúster a una instancia de VDS. En función de la topología que implemente para Supervisor, cree uno o varios grupos de puertos distribuidos. Los grupos de puertos se designan como redes de cargas de trabajo para los espacios de nombres de vSphere.

Las redes de cargas de trabajo proporcionan conectividad a los nodos de los clústeres de Tanzu Kubernetes Grid, a máquinas virtuales creadas usando el servicio de máquina virtual y a máquinas virtuales del plano de control de Supervisor. La red de cargas de trabajo que proporciona conectividad a las máquinas virtuales del plano de control de Kubernetes se denomina red de carga de trabajo principal. Cada Supervisor debe tener una red de cargas de trabajo principal. Debe designar uno de los grupos de puertos distribuidos como la red de cargas de trabajo principal para Supervisor.

Las máquinas virtuales del plano de control de Kubernetes en Supervisor usan tres direcciones IP del rango de direcciones IP que se asigna a la red de cargas de trabajo principal. Cada nodo de un clúster de Tanzu Kubernetes Grid tiene una dirección IP independiente asignada desde el rango de direcciones de la red de cargas de trabajo que está configurada con el espacio de nombres en el que se ejecuta el clúster de Tanzu Kubernetes Grid.

Requisitos de red

El NSX Advanced Load Balancer requiere dos subredes que puedan enrutarse:

- Red de administración. La red de administración es donde reside el Controlador AVI, también denominado Controlador. La red de administración proporciona al controlador conectividad con vCenter Server, hosts ESXi y nodos del plano de control del Supervisor. Esta red es donde se pone la interfaz de administración del motor de servicio de AVI. Esta red requiere un VDS y un grupo de puertos distribuidos.
- Red de datos. La interfaz de datos de los motores de servicio de AVI, también denominados motores de servicio, se conectan a esta red. Las direcciones IP virtuales (VIP) del equilibrador de carga se asignan desde esta red. Esta red requiere una instancia de VDS y grupos de puertos distribuidos. Debe configurar el vDS y los grupos de puertos antes de instalar el equilibrador de carga.

Asignación de direcciones IP

El controlador y el motor de servicios se conectan a la red de administración. Al instalar y configurar NSX Advanced Load Balancer, proporcione una dirección IP estática y enrutable para cada máquina virtual del controlador.

Los motores de servicio pueden utilizar DHCP. Si DHCP no está disponible, puede configurar un grupo de direcciones IP para los motores de servicio.

Colocación de zonas de vSphere en sitios físicos

Puede distribuir las zonas de vSphere entre diferentes sitios físicos siempre que la latencia entre los sitios no supere los 100 ms. Por ejemplo, puede distribuir las zonas de vSphere entre dos sitios físicos: una zona de vSphere en el primer sitio y dos en el segundo sitio.

Requisitos informáticos mínimos para las pruebas

Si desea probar las funcionalidades de vSphere IaaS control plane, puede implementar la plataforma en un cuadro de pruebas muy reducido. Sin embargo, debe tener en cuenta que este tipo de cuadros de pruebas no es adecuado para ejecutar cargas de trabajo de escala de producción y no proporciona HA en el nivel del clúster.

Tabla 5-1. Requisitos informáticos mínimos para las pruebas

<table>
<tr><th>Sistema</th><th>Tamaño de implementación mínimo</th><th>CPU</th><th>Memoria</th><th>Almacenamiento</th></tr>
<tr><td>vCenter Server 8.0</td><td>Pequeño</td><td>2</td><td>21 GB</td><td>290 GB</td></tr>
<tr><td>Clústeres de vSphere</td><td>■ 3 clústeres de vSphere
■ vSphere DRS y HA habilitados en cada clúster de vSphere. vSphere DRS debe estar en el modo Totalmente automatizado o Parcialmente automatizado.
■ Almacenamiento y redes independientes configurados para cada clúster de vSphere.</td><td>No aplicable</td><td>No aplicable</td><td>No aplicable</td></tr>
<tr><td>Hosts ESXi 8.0</td><td>Para cada clúster de vSphere:
■ Sin vSAN: 1 host ESXi con 1 dirección IP estática por host.
■ Con vSAN: 2 hosts ESXi por clúster con al menos 2 NIC físicas.

Nota Asegúrese de que los nombres de los hosts que se unen al clúster utilicen letras minúsculas. De lo contrario, se puede producir un error en la activación del Supervisor.</td><td>8 por host</td><td>64 GB por host</td><td>No aplicable</td></tr>
<tr><td>Máquinas virtuales de plano de control de Kubernetes</td><td>3</td><td>4</td><td>16 GB</td><td>16 GB</td></tr>
<tr><td>Controladora de NSX Advanced Load Balancer</td><td>Enterprise</td><td>4 (Pequeño)
8 (Medio)
24 (Grande)</td><td>12 GB
24 GB
128 GB</td><td>128 GB
128 GB
128 GB</td></tr>
</table>

Requisitos informáticos mínimos para producción

En la tabla se enumeran los requisitos informáticos mínimos para habilitar un Supervisor con redes VDS y NSX Advanced Load Balancer en tres zonas de vSphere. Considere la posibilidad de separar el dominio de administración y el de carga de trabajo como práctica recomendada. El dominio de carga de trabajo aloja el Supervisor donde se ejecutan las cargas de trabajo. El dominio de administración aloja todos los componentes de administración, como vCenter Server.

Tabla 5-2. Requisitos informáticos mínimos

Sistema	Tamaño de implementación mínimo	CPU	Memoria	Almacenamiento
vCenter Server 8.0	Pequeño	2	21 GB	290 GB
Clústeres de vSphere	■ 3 clústeres de vSphere ■ vSphere DRS y HA habilitados en cada clúster de vSphere. vSphere DRS debe estar en el modo Totalmente automatizado o Parcialmente automatizado. ■ Almacenamiento y redes independientes configurados para cada clúster de vSphere.	No aplicable	No aplicable	No aplicable
Hosts ESXi 8.0	Para cada clúster de vSphere: ■ Sin vSAN: 3 hosts ESXi con 1 dirección IP estática por host. ■ Con vSAN: 4 hosts ESXi por clúster con al menos 2 NIC físicas. **Nota** Asegúrese de que los nombres de los hosts que se unen al clúster utilicen letras minúsculas. De lo contrario, se puede producir un error en la habilitación del Supervisor.	8 por host	64 GB por host	No aplicable
Máquinas virtuales de plano de control de Kubernetes	3	4	16 GB	16 GB
Controladora de NSX Advanced Load Balancer	Enterprise Para los entornos de producción, se recomienda instalar un clúster de 3 máquinas virtuales de la controladora. Se requiere un mínimo de 2 máquinas virtuales del motor de servicio para HA.	4 (Pequeño) 8 (Medio) 24 (Grande)	12 GB 24 GB 128 GB	128 GB 128 GB 128 GB

Requisitos mínimos de red

En la tabla se enumeran los requisitos de red mínimos para habilitar un Supervisor con redes VDS y NSX Advanced Load Balancer.

Tabla 5-3. Requisitos de red física

Componente	Cantidad mínima	Configuración necesaria
Dispositivo de capa 2	1	La red de administración que controlará el tráfico de Supervisor debe estar en el mismo dispositivo de capa 2 para todos los clústeres que forman parte del Supervisor. La red de carga de trabajo principal también debe estar en el mismo dispositivo de capa 2.
MTU de red física	1.500	El tamaño de MTU debe ser 1500 o superior en cualquier grupo de puertos distribuidos.

Tabla 5-4. Requisitos de red generales

Componente	Cantidad mínima	Configuración necesaria
Latencia	100 ms	La latencia máxima recomendada entre cada clúster que forma parte de una zona de vSphere unida en un Supervisor.
Servidor NTP y DNS	1	Un servidor DNS y un servidor NTP que se pueden utilizar con vCenter Server. **Nota** Configure NTP en todos los hosts ESXi y vCenter Server.
servidor DHCP	1	Opcional. Configure un servidor DHCP para adquirir automáticamente direcciones IP para las redes de cargas de trabajo y administración, así como direcciones IP flotantes. El servidor DHCP debe admitir identificadores de cliente y proporcionar servidores DNS compatibles, dominios de búsqueda de DNS y un servidor NTP. Para la red de administración, todas las direcciones IP, como las direcciones IP de las máquinas virtuales del plano de control, una IP flotante, servidores DNS, DNS, dominios de búsqueda y servidor NTP, se adquieren automáticamente desde el servidor DHCP. Supervisor utiliza la configuración de DHCP. Los equilibradores de carga pueden requerir direcciones IP estáticas para la administración. Los ámbitos de DHCP no deben superponerse a estas direcciones IP estáticas. DHCP no se utiliza para direcciones IP virtuales. (VIP)

Tabla 5-5. Requisitos de la red de administración

Componente	Cantidad mínima	Configuración necesaria
IP estáticas para las máquinas virtuales del plano de control de Kubernetes	Bloque de 5	Un bloque de 5 direcciones IP estáticas consecutivas que se asignarán desde la red de administración a las máquinas virtuales del plano de control de Kubernetes en el Supervisor.
Red de tráfico de administración	1	Una red de administración que se puede enrutar a los hosts ESXi, a vCenter Server, a la instancia de Supervisor y a un equilibrador de carga.
Subred de red de administración	1	La red de administración es donde reside la controladora de NSX Advanced Load Balancer, también denominada "Controladora". También es donde se conecta la interfaz de administración del motor de servicio. La controladora debe conectarse a las direcciones IP de administración de vCenter Server y ESXi desde esta red **Nota** La red de administración y la red de carga de trabajo deben estar en subredes diferentes. No se admite la asignación de la misma subred a las redes de administración y carga de trabajo, lo que puede provocar errores y problemas en el sistema.

Tabla 5-6. Requisitos de red de cargas de trabajo

Componente	Cantidad mínima	Configuración necesaria
vSphere Distributed Switch	1	Todos los hosts de los tres clústeres de vSphere deben estar conectados a un VDS.
Redes de cargas de trabajo	1	Se debe crear al menos un grupo de puertos distribuidos en la instancia de VDS que se configure como red de cargas de trabajo principal. Según la topología que elija, podrá utilizar el mismo grupo de puertos distribuidos como red de cargas de trabajo de los espacios de nombres o bien podrá crear más grupos de puertos y configurarlos como redes de cargas de trabajo. Las redes de cargas de trabajo deben cumplir los siguientes requisitos: ■ La función de enrutamiento entre las redes de cargas de trabajo con la red que utiliza NSX Advanced Load Balancer para la asignación de direcciones IP virtuales. ■ No hay superposición de los rangos de direcciones IP en todas las redes de cargas de trabajo dentro de Supervisor.
Rango de CIDR de servicios de Kubernetes	/16 direcciones IP privadas	Un rango de CIDR privado para asignar direcciones IP a los servicios de Kubernetes. Debe especificar un rango de CIDR único de servicios de Kubernetes para cada Supervisor.

Tabla 5-7. Requisitos de red del equilibrador de carga

Servidor NTP y DNS	1	La IP del servidor DNS es necesaria para que la controladora de NSX Advanced Load Balancer resuelva correctamente los nombres de host de vCenter Server y ESXi. NTP es opcional, ya que los servidores NTP públicos se utilizan de forma predeterminada.
Subred de red de datos	1	La interfaz de datos de los motores de servicio, también denominados "motores de servicio", se conectan a esta red. Configure un grupo de direcciones IP para los motores de servicio. Las direcciones IP virtuales (VIP) del equilibrador de carga se asignan desde esta red.
IP de la controladora de NSX Advanced Load Balancer	1 o 4	Si implementa la controladora de NSX Advanced Load Balancer como un solo nodo, se requiere una dirección IP estática para su interfaz de administración. Para un clúster de 3 nodos, se requieren 4 direcciones IP . Una para cada máquina virtual de la controladora y otra para la VIP del clúster. Estas direcciones IP deben proceder de la subred de la red de administración.
Rango de VIP de IPAM	-	Un rango de CIDR privado para asignar direcciones IP a los servicios de Kubernetes. Las direcciones IP deben proceder de la subred de la red de datos. Debe especificar un rango de CIDR de servicios de Kubernetes único para cada clúster supervisor.

Puertos y protocolos

En esta tabla se especifican los protocolos y los puertos necesarios para administrar la conectividad IP entre NSX Advanced Load Balancer, vCenter Server y otros componentes de vSphere IaaS control plane.

Origen	Destino	Protocolo y puertos
Controladora de NSX Advanced Load Balancer	Controladora de NSX Advanced Load Balancer (en el clúster)	TCP 22 (SSH) TCP 443 (HTTPS) TCP 8443 (HTTPS)
Motor de servicio	Engine de servicio en HA	TCP 9001 para VMware, LSC y NSX-T Cloud
Motor de servicio	Controladora de NSX Advanced Load Balancer	TCP 22 (SSH) TCP 8443 (HTTPS) TCP 123 (NTP)
Controladora de NSX Advanced Load Balancer	vCenter Server, ESXi, NSX-T Manager	TCP 443 (HTTPS)
Nodos del plano de control de supervisor (AKO)	Controladora de NSX Advanced Load Balancer	TCP 443 (HTTPS)

Para obtener más información sobre los puertos y los protocolos de NSX Advanced Load Balancer, consulte https://ports.esp.vmware.com/home/NSX-Advanced-Load-Balancer.

Requisitos para Supervisor zonal con NSX

Consulte los requisitos del sistema para habilitar un Supervisor en tres clústeres de vSphere asignados a zonas de vSphere mediante la pila de redes de NSX.

Además de estos requisitos, consulte la Guía de diseño de referencia de NSX para obtener más información sobre las prácticas recomendadas para implementar NSX.

Colocación de zonas de vSphere en sitios físicos

Puede distribuir las zonas de vSphere entre diferentes sitios físicos siempre que la latencia entre los sitios no supere los 100 ms. Por ejemplo, puede distribuir las zonas de vSphere entre dos sitios físicos: una zona de vSphere en el primer sitio y dos en el segundo sitio.

Requisitos informáticos mínimos para un clúster de Edge y administración

Sistema	Tamaño de implementación mínimo	CPU	Memoria	Almacenamiento
vCenter Server 8	Pequeño	2	21 GB	290 GB
8 hosts ESXi	2 hosts ESXi	8	64 GB por host	No aplicable
NSX Manager	Mediano	6	24 GB	300 GB

Sistema	Tamaño de implementación mínimo	CPU	Memoria	Almacenamiento
NSX Edge 1	Grande	8	32 GB	200 GB
NSX Edge 2	Grande	8	32 GB	200 GB

Nota Compruebe que todos los hosts ESXi que participan en el clúster de vSphere en el que tiene pensado configurar vSphere IaaS control plane estén preparados como nodos de transporte de NSX. Para obtener más información, consulte https://kb.vmware.com/s/article/95820 y Preparar hosts ESXi como nodos de transporte en la documentación de NSX.

Requisitos informáticos mínimos para clústeres de dominio de carga de trabajo

Sistema	Tamaño de implementación mínimo	CPU	Memoria	Almacenamiento
Clústeres de vSphere	■ 3 clústeres de vSphere ■ vSphere DRS y HA habilitados en cada clúster de vSphere. vSphere DRS debe estar en el modo Totalmente automatizado. ■ Almacenamiento y redes independientes configurados para cada clúster de vSphere.	No aplicable	No aplicable	No aplicable
8 hosts ESXi	Para cada clúster de vSphere: ■ Sin vSAN: 3 hosts ESXi con 1 dirección IP estática por host. ■ Con vSAN: 4 hosts ESXi por clúster con al menos 2 NIC físicas. **Nota** Asegúrese de que los nombres de los hosts que se unen a los clústeres utilicen letras minúsculas. De lo contrario, se puede producir un error en la activación del Supervisor.	8	64 GB por host	No aplicable
Máquinas virtuales de plano de control de Kubernetes	3	4	16 GB	16 GB

Requisitos de red

Nota No puede crear clústeres IPv6 con un Supervisor de vSphere 8 ni registrar clústeres IPv6 con Tanzu Mission Control.

Compruebe la Matriz de interoperabilidad de productos VMware para conocer las versiones de NSX compatibles.

Tabla 5-8. Requisitos de red física

Componente	Cantidad mínima	Configuración necesaria
Dispositivo de capa 2	1	La red de administración que controlará el tráfico de Supervisor debe estar en el mismo dispositivo de capa 2. Al menos una NIC física por host que maneja el tráfico de administración debe estar conectada a ese dispositivo de capa 2.
MTU de red física	1.500	El tamaño de MTU debe ser 1500 o superior en cualquier grupo de puertos de vSphere Distributed Switch.
NIC física	Al menos 2 NIC físicas por host si se utiliza vSAN	Para utilizar la CNI de Antrea y obtener un rendimiento de NSX óptimo, cada NIC física en cada host ESXi participante debe admitir la encapsulación GENEVE y debe tenerla habilitada.

Tabla 5-9. Requisitos de red generales

Componente	Cantidad mínima	Configuración necesaria
Latencia	100 ms	La latencia máxima recomendada entre cada clúster que forma parte de una zona de vSphere unida en un Supervisor.
Servidor NTP y DNS	1	Un servidor DNS y un servidor NTP que se pueden utilizar con vCenter Server. **Nota** Configure NTP en todos los hosts ESXi y vCenter Server.

Tabla 5-9. Requisitos de red generales (continuación)

Componente	Cantidad mínima	Configuración necesaria
servidor DHCP	1	Opcional. Configure un servidor DHCP para adquirir automáticamente direcciones IP para las redes de administración y cargas de trabajo, así como direcciones IP flotantes. El servidor DHCP debe admitir identificadores de cliente y proporcionar servidores DNS compatibles, dominios de búsqueda de DNS y un servidor NTP. Para la red de administración, todas las direcciones IP, como las direcciones IP de las máquinas virtuales del plano de control, una IP flotante, servidores DNS, DNS, dominios de búsqueda y servidor NTP, se adquieren automáticamente desde el servidor DHCP. Supervisor utiliza la configuración de DHCP. Los equilibradores de carga pueden requerir direcciones IP estáticas para la administración. Los ámbitos de DHCP no deben superponerse a estas direcciones IP estáticas. DHCP no se utiliza para direcciones IP virtuales. (VIP)
Registro de imágenes	1	Acceda a un registro para el servicio.

Tabla 5-10. Requisitos de la red de administración

Componente	Cantidad mínima	Configuración necesaria
IP estáticas para las máquinas virtuales del plano de control de Kubernetes	Bloque de 5	Un bloque de 5 direcciones IP estáticas consecutivas que se asignarán desde la red de administración a las máquinas virtuales del plano de control de Kubernetes en el Supervisor.
Red de tráfico de administración	1	Una red de administración que se puede enrutar a los hosts ESXi, a vCenter Server, a la instancia de Supervisor y a un equilibrador de carga.

Tabla 5-10. Requisitos de la red de administración (continuación)

Componente	Cantidad mínima	Configuración necesaria
Subred de red de administración	1	La subred que se utiliza para el tráfico de administración entre los hosts ESXi y vCenter Server, las instancias de NSX Appliance y el plano de control de Kubernetes. El tamaño de la subred debe ser el siguiente: ■ Una dirección IP por adaptador de VMkernel de host. ■ Una dirección IP para vCenter Server Appliance. ■ Una o cuatro direcciones IP para NSX Manager. Cuatro cuando se realiza una agrupación de NSX Manager de 3 nodos y 1 IP virtual (VIP). ■ 5 direcciones IP para el plano de control de Kubernetes. 1 para cada uno de los 3 nodos, 1 para la IP virtual, 1 para la actualización sucesiva de clústeres. **Nota** La red de administración y la red de carga de trabajo deben estar en subredes diferentes. No se admite la asignación de la misma subred a las redes de administración y carga de trabajo, lo que puede provocar errores y problemas en el sistema.
VLAN de red de administración	1	Identificador de VLAN de la subred de la red de administración.

Tabla 5-11. Requisitos de red de cargas de trabajo

Componente	Cantidad mínima	Configuración necesaria
Rango de CIDR del pod de vSphere	/23 direcciones IP privadas	Un rango de CIDR privado que proporciona direcciones IP a los pods de vSphere. Estas direcciones también se utilizan para los nodos del clúster de Tanzu Kubernetes Grid. Debe especificar un rango de CIDR único del pod de vSphere para cada clúster. **Nota** El rango de CIDR del pod de vSphere y el rango de CIDR de las direcciones del servicio de Kubernetes no deben superponerse.
Rango de CIDR de servicios de Kubernetes	/16 direcciones IP privadas	Un rango de CIDR privado para asignar direcciones IP a los servicios de Kubernetes. Debe especificar un rango de CIDR único de servicios de Kubernetes para cada Supervisor.
Rango de CIDR de salida	/27 direcciones IP estáticas	Una anotación de CIDR privado para determinar la IP de egreso de los servicios de Kubernetes. Solo se asigna una dirección IP de egreso para cada espacio de nombres en el Supervisor. La IP de egreso es la dirección que las entidades externas utilizan para comunicarse con los servicios en el espacio de nombres. La cantidad de direcciones IP de egreso limita el número de directivas de egreso que puede tener el Supervisor. El valor mínimo es un CIDR de /27 o más. Por ejemplo, `10.174.4.96/27` **Nota** Las direcciones IP de egreso y las direcciones IP de entrada no deben superponerse.

Tabla 5-11. Requisitos de red de cargas de trabajo (continuación)

Componente	Cantidad mínima	Configuración necesaria
CIDR de entrada	/27 direcciones IP estáticas	Un rango de CIDR privado que se utilizará para las direcciones IP de entradas. La entrada permite aplicar directivas de tráfico a las solicitudes que entran en Supervisor desde redes externas. La cantidad de direcciones IP de entrada limita el número de entradas que puede tener el clúster. El valor mínimo es un CIDR de /27 o más. **Nota** Las direcciones IP de egreso y las direcciones IP de entrada no deben superponerse.
Rango de redes de espacio de nombres	1	Uno o varios CIDR de IP para crear subredes o segmentos y asignar direcciones IP a las cargas de trabajo.
Prefijo de subred de espacio de nombres	1	El prefijo de subred que especifica el tamaño de la subred reservada para segmentos de espacios de nombres. El valor predeterminado es 28.

Tabla 5-12. Requisitos de NSX

Componente	Cantidad mínima	V
VLAN	3	Las IP de VLAN son las direcciones IP de los endpoints de túnel (Tunnel Endpoints, TEP). Los TEP del host ESXi y los TEP de Edge deben ser enrutables. Las direcciones IP de VLAN son necesarias para lo siguiente: ■ VTEP de host ESXi ■ VTEP de Edge con la IP estática ■ Puerta de enlace de nivel 0 y vínculo superior para el nodo de transporte. **Nota** El VTEP del host ESXi y el VTEP de Edge deben tener un tamaño de MTU superior a 1600. Los hosts ESXi y los nodos de NSX-T Edge actúan como endpoints de túnel y se asigna una IP de endpoint de túnel (Tunnel Endpoint, TEP) a cada nodo de Edge y host. Como las IP de TEP para hosts ESXi crean un túnel de superposición con IP de TEP en los nodos de Edge, las IP de VLAN deben poder enrutarse. Se requiere una VLAN adicional para proporcionar conectividad de norte a sur a la puerta de enlace de nivel 0. Los grupos de direcciones IP pueden compartirse entre clústeres. Sin embargo, el grupo de direcciones IP/VLAN de superposición de host no se debe compartir con la VLAN o el grupo de direcciones IP de superposición de Edge. **Nota** Si el TEP del host y el TEP de Edge usan diferentes NIC físicas, pueden utilizar la misma VLAN.
IP de vínculo superior de nivel 0	/24 direcciones IP privadas	La subred de IP que se utiliza para el vínculo superior de nivel 0. Los requisitos para la dirección IP del vínculo superior de nivel 0 son los siguientes: ■ 1 dirección IP, si no se requiere redundancia de Edge. ■ 4 direcciones IP; si utiliza BGP y redundancia de Edge, necesitará 2 direcciones IP por Edge. ■ 3 direcciones IP, si utiliza rutas estáticas y redundancia de Edge. La IP de administración de Edge, la subred, la puerta de enlace, la IP de vínculo superior, la subred y la puerta de enlace deben ser únicas.

Requisitos para Supervisor zonal con NSX y NSX Advanced Load Balancer

Consulte los requisitos del sistema para habilitar un Supervisor en tres clústeres de vSphere asignados a zonas de vSphere mediante la pila de redes de NSX y NSX Advanced Load Balancer.

Colocación de zonas de vSphere en sitios físicos

Puede distribuir las zonas de vSphere entre diferentes sitios físicos siempre que la latencia entre los sitios no supere los 100 ms. Por ejemplo, puede distribuir las zonas de vSphere entre dos sitios físicos: una zona de vSphere en el primer sitio y dos en el segundo sitio.

Opciones de implementación de NSX

Para obtener más información sobre las prácticas recomendadas para implementar NSX, consulte Guía de diseño de referencia de NSX.

Requisitos informáticos mínimos para un clúster de Edge y administración

Sistema	Tamaño de implementación mínimo	CPU	Memoria	Almacenamiento
vCenter Server 8	Pequeño	2	21 GB	290 GB
8 hosts ESXi	2 hosts ESXi	8	64 GB por host	No aplicable
NSX Manager	Mediano	6	24 GB	300 GB
NSX Edge 1	Grande	8	32 GB	200 GB
NSX Edge 2	Grande	8	32 GB	200 GB
Máquinas virtuales del motor de servicio	Se implementan al menos dos máquinas virtuales del motor de servicio por Supervisor	1	2 GB	N/C

Nota Compruebe que todos los hosts ESXi que participan en el clúster de vSphere en el que tiene pensado configurar vSphere IaaS control plane estén preparados como nodos de transporte de NSX. Para obtener más información, consulte https://kb.vmware.com/s/article/95820 y Preparar hosts ESXi como nodos de transporte en la documentación de NSX.

Especificar la capacidad del sistema del controlador

Puede especificar la capacidad del sistema del controlador durante la implementación. La capacidad del sistema se basa en asignaciones de recursos del sistema, como CPU, RAM y disco. La cantidad de recursos que asigne tiene un impacto en el rendimiento del controlador.

Tipo de implementación	Recuento de nodos	Asignaciones recomendadas: CPU	Asignaciones recomendadas: memoria	Asignaciones recomendadas: disco
Demostración/ Evaluación del cliente	1	6	24 GB	128 GB

En las implementaciones de demostración, con un único controlador es suficiente y se utiliza para todas las actividades y los flujos de trabajo del plano de control, así como para los análisis.

En una implementación de producción, se recomienda un clúster de tres nodos.

Para obtener más información, consulte Tamaño del controlador de NSX Advanced Load Balancer.

Requisitos informáticos mínimos para clústeres de dominio de carga de trabajo

Sistema	Tamaño de implementación mínimo	CPU	Memoria	Almacenamiento
Clústeres de vSphere	■ 3 clústeres de vSphere ■ vSphere DRS y HA habilitados en cada clúster de vSphere. vSphere DRS debe estar en el modo Totalmente automatizado. ■ Almacenamiento y redes independientes configurados para cada clúster de vSphere.	No aplicable	No aplicable	No aplicable
8 hosts ESXi	Para cada clúster de vSphere: ■ Sin vSAN: 3 hosts ESXi con 1 dirección IP estática por host. ■ Con vSAN: 4 hosts ESXi por clúster con al menos 2 NIC físicas. **Nota** Asegúrese de que los nombres de los hosts que se unen a los clústeres utilicen letras minúsculas. De lo contrario, se puede producir un error en la activación del Supervisor.	8	64 GB por host	No aplicable
Máquinas virtuales de plano de control de Kubernetes	3	4	16 GB	16 GB

Requisitos de red

Nota No puede crear clústeres IPv6 con un Supervisor de vSphere 8 ni registrar clústeres IPv6 con Tanzu Mission Control.

Compruebe la Matriz de interoperabilidad de productos VMware para conocer las versiones de NSX compatibles.

Tabla 5-13. Requisitos de red física

Componente	Cantidad mínima	Configuración necesaria
Dispositivo de capa 2	1	La red de administración que controlará el tráfico de Supervisor debe estar en el mismo dispositivo de capa 2. Al menos una NIC física por host que maneja el tráfico de administración debe estar conectada a ese dispositivo de capa 2.
MTU de red física	1700	El tamaño de MTU debe ser 1700 o superior en cualquier grupo de puertos de vSphere Distributed Switch.
NIC física	Al menos 2 NIC físicas por host si se utiliza vSAN	Para utilizar la CNI de Antrea y obtener un rendimiento de NSX óptimo, cada NIC física en cada host ESXi participante debe admitir la encapsulación GENEVE y debe tenerla habilitada.

Tabla 5-14. Requisitos de red generales

Componente	Cantidad mínima	Configuración necesaria
Latencia	100 ms	La latencia máxima recomendada entre cada clúster que forma parte de una zona de vSphere unida en un Supervisor.
Servidor NTP y DNS	1	Un servidor DNS y un servidor NTP que se pueden utilizar con vCenter Server. **Nota** Configure NTP en todos los hosts ESXi y vCenter Server.

Tabla 5-14. Requisitos de red generales (continuación)

Componente	Cantidad mínima	Configuración necesaria
servidor DHCP	1	Opcional. Configure un servidor DHCP para adquirir automáticamente direcciones IP para las redes de administración y cargas de trabajo, así como direcciones IP flotantes. El servidor DHCP debe admitir identificadores de cliente y proporcionar servidores DNS compatibles, dominios de búsqueda de DNS y un servidor NTP. Para la red de administración, todas las direcciones IP, como las direcciones IP de las máquinas virtuales del plano de control, una IP flotante, servidores DNS, DNS, dominios de búsqueda y servidor NTP, se adquieren automáticamente desde el servidor DHCP. Supervisor utiliza la configuración de DHCP. Los equilibradores de carga pueden requerir direcciones IP estáticas para la administración. Los ámbitos de DHCP no deben superponerse a estas direcciones IP estáticas. DHCP no se utiliza para direcciones IP virtuales. (VIP)
Registro de imágenes	1	Acceda a un registro para el servicio.

Tabla 5-15. Requisitos de la red de administración

Componente	Cantidad mínima	Configuración necesaria
IP estáticas para las máquinas virtuales del plano de control de Kubernetes	Bloque de 5	Un bloque de 5 direcciones IP estáticas consecutivas que se asignarán desde la red de administración a las máquinas virtuales del plano de control de Kubernetes en el Supervisor.
Red de tráfico de administración	1	Una red de administración que se puede enrutar a los hosts ESXi, a vCenter Server, a la instancia de Supervisor y a un equilibrador de carga.

Tabla 5-15. Requisitos de la red de administración (continuación)

Componente	Cantidad mínima	Configuración necesaria
Subred de red de administración	1	La subred que se utiliza para el tráfico de administración entre los hosts ESXi y vCenter Server, las instancias de NSX Appliance y el plano de control de Kubernetes. El tamaño de la subred debe ser el siguiente: ■ Una dirección IP por adaptador de VMkernel de host. ■ Una dirección IP para vCenter Server Appliance. ■ Una o cuatro direcciones IP para NSX Manager. Cuatro cuando se realiza una agrupación de NSX Manager de 3 nodos y 1 IP virtual (VIP). ■ 5 direcciones IP para el plano de control de Kubernetes. 1 para cada uno de los 3 nodos, 1 para la IP virtual, 1 para la actualización sucesiva de clústeres. **Nota** La red de administración y la red de carga de trabajo deben estar en subredes diferentes. No se admite la asignación de la misma subred a las redes de administración y carga de trabajo, lo que puede provocar errores y problemas en el sistema.
VLAN de red de administración	1	Identificador de VLAN de la subred de la red de administración.

Tabla 5-16. Requisitos de red de cargas de trabajo

Componente	Cantidad mínima	Configuración necesaria
Rango de CIDR del pod de vSphere	/23 direcciones IP privadas	Un rango de CIDR privado que proporciona direcciones IP a los pods de vSphere. Estas direcciones también se utilizan para los nodos del clúster de Tanzu Kubernetes Grid. Debe especificar un rango de CIDR único del pod de vSphere para cada clúster. **Nota** El rango de CIDR del pod de vSphere y el rango de CIDR de las direcciones del servicio de Kubernetes no deben superponerse.
Rango de CIDR de servicios de Kubernetes	/16 direcciones IP privadas	Un rango de CIDR privado para asignar direcciones IP a los servicios de Kubernetes. Debe especificar un rango de CIDR único de servicios de Kubernetes para cada Supervisor.
Rango de CIDR de salida	/27 direcciones IP estáticas	Una anotación de CIDR privado para determinar la IP de egreso de los servicios de Kubernetes. Solo se asigna una dirección IP de egreso para cada espacio de nombres en el Supervisor. La IP de egreso es la dirección que las entidades externas utilizan para comunicarse con los servicios en el espacio de nombres. La cantidad de direcciones IP de egreso limita el número de directivas de egreso que puede tener el Supervisor. El valor mínimo es un CIDR de /27 o más. Por ejemplo, `10.174.4.96/27` **Nota** Las direcciones IP de egreso y las direcciones IP de entrada no deben superponerse.

Tabla 5-16. Requisitos de red de cargas de trabajo (continuación)

Componente	Cantidad mínima	Configuración necesaria
CIDR de entrada	/27 direcciones IP estáticas	Un rango de CIDR privado que se utilizará para las direcciones IP de entradas. La entrada permite aplicar directivas de tráfico a las solicitudes que entran en Supervisor desde redes externas. La cantidad de direcciones IP de entrada limita el número de entradas que puede tener el clúster. El valor mínimo es un CIDR de /27 o más. **Nota** Las direcciones IP de egreso y las direcciones IP de entrada no deben superponerse.
Rango de redes de espacio de nombres	1	Uno o varios CIDR de IP para crear subredes o segmentos y asignar direcciones IP a las cargas de trabajo.
Prefijo de subred de espacio de nombres	1	El prefijo de subred que especifica el tamaño de la subred reservada para segmentos de espacios de nombres. El valor predeterminado es 28.

Tabla 5-17. Requisitos de NSX

<table>
<tr><th>Componente</th><th>Cantidad mínima</th><th>V</th></tr>
<tr><td>VLAN</td><td>3</td><td>Las IP de VLAN son las direcciones IP de los endpoints de túnel (Tunnel Endpoints, TEP). Los TEP del host ESXi y los TEP de Edge deben ser enrutables.
Las direcciones IP de VLAN son necesarias para lo siguiente:
■ VTEP de host ESXi
■ VTEP de Edge con la IP estática
■ Puerta de enlace de nivel 0 y vínculo superior para el nodo de transporte.
Nota El VTEP del host ESXi y el VTEP de Edge deben tener un tamaño de MTU superior a 1600.
Los hosts ESXi y los nodos de NSX-T Edge actúan como endpoints de túnel y se asigna una IP de endpoint de túnel (Tunnel Endpoint, TEP) a cada nodo de Edge y host.
Como las IP de TEP para hosts ESXi crean un túnel de superposición con IP de TEP en los nodos de Edge, las IP de VLAN deben poder enrutarse.
Se requiere una VLAN adicional para proporcionar conectividad de norte a sur a la puerta de enlace de nivel 0.
Los grupos de direcciones IP pueden compartirse entre clústeres. Sin embargo, el grupo de direcciones IP/VLAN de superposición de host no se debe compartir con la VLAN o el grupo de direcciones IP de superposición de Edge.
Nota Si el TEP del host y el TEP de Edge usan diferentes NIC físicas, pueden utilizar la misma VLAN.</td></tr>
<tr><td>IP de vínculo superior de nivel 0</td><td>/24 direcciones IP privadas</td><td>La subred de IP que se utiliza para el vínculo superior de nivel 0. Los requisitos para la dirección IP del vínculo superior de nivel 0 son los siguientes:
■ 1 dirección IP, si no se requiere redundancia de Edge.
■ 4 direcciones IP; si utiliza BGP y redundancia de Edge, necesitará 2 direcciones IP por Edge.
■ 3 direcciones IP, si utiliza rutas estáticas y redundancia de Edge.
La IP de administración de Edge, la subred, la puerta de enlace, la IP de vínculo superior, la subred y la puerta de enlace deben ser únicas.</td></tr>
</table>

Tabla 5-18. Requisitos de red del equilibrador de carga

Servidor NTP y DNS	1	La IP del servidor DNS es necesaria para que la controladora de NSX Advanced Load Balancer resuelva correctamente los nombres de host de vCenter Server y ESXi. NTP es opcional, ya que los servidores NTP públicos se utilizan de forma predeterminada.
Subred de red de datos	1	La interfaz de datos de los motores de servicio, también denominados "motores de servicio", se conectan a esta red. Configure un grupo de direcciones IP para los motores de servicio. Las direcciones IP virtuales (VIP) del equilibrador de carga se asignan desde esta red.
IP de la controladora de NSX Advanced Load Balancer	1 o 4	Si implementa la controladora de NSX Advanced Load Balancer como un solo nodo, se requiere una dirección IP estática para su interfaz de administración. Para un clúster de 3 nodos, se requieren 4 direcciones IP . Una para cada máquina virtual de la controladora y otra para la VIP del clúster. Estas direcciones IP deben proceder de la subred de la red de administración.
Rango de VIP de IPAM	-	Un rango de CIDR privado para asignar direcciones IP a los servicios de Kubernetes. Las direcciones IP deben proceder de la subred de la red de datos. Debe especificar un rango de CIDR de servicios de Kubernetes único para cada clúster supervisor.

Puertos y protocolos

En esta tabla se especifican los protocolos y los puertos necesarios para administrar la conectividad IP entre NSX Advanced Load Balancer, vCenter Server y otros componentes de vSphere IaaS control plane.

Origen	Destino	Protocolo y puertos
Controladora de NSX Advanced Load Balancer	Controladora de NSX Advanced Load Balancer (en el clúster)	TCP 22 (SSH) TCP 443 (HTTPS) TCP 8443 (HTTPS)
Motor de servicio	Engine de servicio en HA	TCP 9001 para VMware, LSC y NSX-T Cloud
Motor de servicio	Controladora de NSX Advanced Load Balancer	TCP 22 (SSH) TCP 8443 (HTTPS) TCP 123 (NTP)
Controladora de NSX Advanced Load Balancer	vCenter Server, ESXi, NSX-T Manager	TCP 443 (HTTPS)
Nodos del plano de control de supervisor (AKO)	Controladora de NSX Advanced Load Balancer	TCP 443 (HTTPS)

Para obtener más información sobre los puertos y los protocolos de NSX Advanced Load Balancer, consulte https://ports.esp.vmware.com/home/NSX-Advanced-Load-Balancer.

Requisitos para la implementación de un Supervisor zonal con equilibrador de carga de HAProxy

Revise los requisitos para habilitar un Supervisor con redes VDS y equilibrador de carga de HAProxy en tres clústeres de vSphere asignados a zonas de vSphere.

Colocación de zonas de vSphere en sitios físicos

Puede distribuir las zonas de vSphere entre diferentes sitios físicos siempre que la latencia entre los sitios no supere los 100 ms. Por ejemplo, puede distribuir las zonas de vSphere entre dos sitios físicos: una zona de vSphere en el primer sitio y dos en el segundo sitio.

Requisitos informáticos mínimos

En la tabla se enumeran los requisitos informáticos mínimos para habilitar un Supervisor con redes VDS y un equilibrador de carga de HAProxy en tres zonas de vSphere. Considere la posibilidad de separar el dominio de administración y el de carga de trabajo como práctica recomendada. El dominio de carga de trabajo aloja el Supervisor donde se ejecutan las cargas de trabajo. El dominio de administración aloja todos los componentes de administración, como vCenter Server.

Sistema	Tamaño de implementación mínimo	CPU	Memoria	Almacenamiento
vCenter Server 8.0	Pequeño	2	21 GB	290 GB
Clústeres de vSphere	■ 3 clústeres de vSphere ■ vSphere DRS y HA habilitados en cada clúster de vSphere. vSphere DRS debe estar en el modo Totalmente automatizado o Parcialmente automatizado. ■ Almacenamiento y redes independientes configurados para cada clúster de vSphere.	No aplicable	No aplicable	No aplicable
Hosts ESXi 8.0	Para cada clúster de vSphere: ■ Sin vSAN: 3 hosts ESXi con 1 dirección IP estática por host ■ Con vSAN: 4 hosts ESXi por clúster con al menos 2 NIC físicas. **Nota** Asegúrese de que los nombres de los hosts que se unen a los clústeres utilicen letras minúsculas. De lo contrario, se puede producir un error en la habilitación del Supervisor.	8	64 GB por host	No aplicable
Máquinas virtuales de plano de control de Kubernetes	3	4	16 GB	16 GB

Requisitos mínimos de red

Nota No puede crear clústeres IPv6 con un Supervisor de vSphere 8 ni registrar clústeres IPv6 con Tanzu Mission Control.

Tabla 5-19. Requisitos de red física

Componente	Cantidad mínima	Configuración necesaria
Dispositivo de capa 2	1	La red de administración que controlará el tráfico de Supervisor debe estar en el mismo dispositivo de capa 2 para todos los clústeres que forman parte del Supervisor. La red de carga de trabajo principal también debe estar en el mismo dispositivo de capa 2.
MTU de red física	1.500	El tamaño de MTU debe ser 1500 o superior en cualquier grupo de puertos distribuidos.

Tabla 5-20. Requisitos de red generales

Componente	Cantidad mínima	Configuración necesaria
Latencia	100 ms	La latencia máxima recomendada entre cada clúster que forma parte de una zona de vSphere unida en un Supervisor.
Servidor NTP y DNS	1	Un servidor DNS y un servidor NTP que se pueden utilizar con vCenter Server. **Nota** Configure NTP en todos los hosts ESXi y vCenter Server.
servidor DHCP	1	Opcional. Configure un servidor DHCP para adquirir automáticamente direcciones IP para las redes de administración y cargas de trabajo, así como direcciones IP flotantes. El servidor DHCP debe admitir identificadores de cliente y proporcionar servidores DNS compatibles, dominios de búsqueda de DNS y un servidor NTP. Para la red de administración, todas las direcciones IP, como las direcciones IP de las máquinas virtuales del plano de control, una IP flotante, servidores DNS, DNS, dominios de búsqueda y servidor NTP, se adquieren automáticamente desde el servidor DHCP. Supervisor utiliza la configuración de DHCP. Los equilibradores de carga pueden requerir direcciones IP estáticas para la administración. Los ámbitos de DHCP no deben superponerse a estas direcciones IP estáticas. DHCP no se utiliza para direcciones IP virtuales. (VIP)

Tabla 5-21. Requisitos de la red de administración

Componente	Cantidad mínima	Configuración necesaria
IP estáticas para las máquinas virtuales del plano de control de Kubernetes	Bloque de 5	Un bloque de 5 direcciones IP estáticas consecutivas que se asignarán desde la red de administración a las máquinas virtuales del plano de control de Kubernetes en el Supervisor.
Red de tráfico de administración	1	Una red de administración que se puede enrutar a los hosts ESXi, a vCenter Server, a la instancia de Supervisor y a un equilibrador de carga.
Subred de red de administración	1	La subred que se utiliza para el tráfico de administración entre los hosts ESXi y vCenter Server y el plano de control de Kubernetes. El tamaño de la subred debe ser el siguiente: ■ Una dirección IP por adaptador de VMkernel de host. ■ Una dirección IP para vCenter Server Appliance. ■ 5 direcciones IP para el plano de control de Kubernetes. 1 para cada uno de los 3 nodos, 1 para la IP virtual, 1 para la actualización sucesiva de clústeres. **Nota** La red de administración y la red de carga de trabajo deben estar en subredes diferentes. No se admite la asignación de la misma subred a las redes de administración y carga de trabajo, lo que puede provocar errores y problemas en el sistema.
VLAN de red de administración	1	Identificador de VLAN de la subred de la red de administración.

Tabla 5-22. Requisitos de red de cargas de trabajo

Componente	Cantidad mínima	Configuración necesaria
vSphere Distributed Switch	1	Todos los hosts de los tres clústeres de vSphere deben estar conectados a un VDS.
Redes de cargas de trabajo	1	Se debe crear al menos un grupo de puertos distribuidos en la instancia de VDS que se configure como red de cargas de trabajo principal. Según la topología que elija, podrá utilizar el mismo grupo de puertos distribuidos como red de cargas de trabajo de los espacios de nombres o bien podrá crear más grupos de puertos y configurarlos como redes de cargas de trabajo. Las redes de cargas de trabajo deben cumplir los siguientes requisitos: ■ La función de enrutamiento entre las redes de cargas de trabajo con la red que utiliza HAProxy para la asignación de direcciones IP virtuales. ■ No hay superposición de los rangos de direcciones IP en todas las redes de cargas de trabajo dentro de Supervisor. **Importante** La red de carga de trabajo debe estar en una subred diferente a la red de administración.
Rango de CIDR de servicios de Kubernetes	/16 direcciones IP privadas	Un rango de CIDR privado para asignar direcciones IP a los servicios de Kubernetes. Debe especificar un rango de CIDR único de servicios de Kubernetes para cada Supervisor.

Tabla 5-23. Requisitos de red del equilibrador de carga

Equilibrador de carga de HAProxy	1	Una instancia del equilibrador de carga de HAProxy configurada con la instancia de vCenter Server. ■ Si la misma instancia de HAProxy atiende a varios Supervisores debe poder enrutar el tráfico que se dirige a todas las redes de cargas de trabajo y el tráfico que procede de ellas en todos los Supervisores. ■ Los rangos de direcciones IP en las redes de cargas de trabajo en todos los Supervisores a los que atiende HAProxy no deben superponerse. ■ La red que utiliza HAProxy para asignar direcciones IP virtuales debe enrutarse a las redes de cargas de trabajo que se utilizan en todos los Supervisores a los que se conecta HAProxy.
Rango de IP del servidor virtual	1	Un rango de IP dedicado para direcciones IP virtuales. La máquina virtual de HAProxy debe ser el único propietario de este rango de IP virtual. El rango no debe superponerse con ningún otro rango de IP asignado a alguna red de cargas de trabajo que sea propiedad de una instancia de Supervisor. El rango no debe residir en la misma subred que la red de administración.

Requisitos para la implementación de clústeres de Supervisor

6

Revise los requisitos para habilitar un Supervisor en un clúster único de vSphere que se asigna a una zona de vSphere.

Lea los siguientes temas a continuación:

- Requisitos para la implementación de clústeres de Supervisor con redes VDS y NSX Advanced Load Balancer
- Requisitos para la implementación de clústeres de Supervisor con NSX
- Requisitos para la implementación de Supervisor del clúster con NSX y NSX Advanced Load Balancer
- Requisitos para la implementación de clústeres de Supervisor con redes VDS y equilibrador de carga de HAProxy

Requisitos para la implementación de clústeres de Supervisor con redes VDS y NSX Advanced Load Balancer

Compruebe los requisitos para habilitar un Supervisor en un clúster de vSphere con redes vDS y NSX Advanced Load Balancer, también conocido como equilibrador de carga AVI. vSphere IaaS control plane admite varias topologías: una única red de vDS para los servicios del motor de servicio de AVI y del equilibrador de carga, y un vDS para el plano de administración de AVI y otro vDS para el NSX Advanced Load Balancer.

Redes de cargas de trabajo

Para configurar una instancia de Supervisor con la pila de redes vDS, debe conectar todos los hosts del clúster a una instancia de vDS. En función de la topología que implemente para Supervisor, cree uno o varios grupos de puertos distribuidos. Los grupos de puertos se designan como redes de cargas de trabajo para los espacios de nombres de vSphere. Las redes de cargas de trabajo proporcionan conectividad a los nodos de los clústeres de Tanzu Kubernetes Grid y a las máquinas virtuales del plano de control de Supervisor. La red de cargas de trabajo que proporciona conectividad a las máquinas virtuales del plano de control de Kubernetes se denomina red de carga de trabajo principal. Cada Supervisor debe tener una red de cargas de trabajo principal. Debe designar uno de los grupos de puertos distribuidos como la red de cargas de trabajo principal para Supervisor.

Las máquinas virtuales del plano de control de Kubernetes en Supervisor usan tres direcciones IP del rango de direcciones IP que se asigna a la red de cargas de trabajo principal. Cada nodo de un clúster de Tanzu Kubernetes Grid tiene una dirección IP independiente asignada desde el rango de direcciones de la red de cargas de trabajo que está configurada con el espacio de nombres en el que se ejecuta el clúster de Tanzu Kubernetes Grid.

Requisitos de red

El NSX Advanced Load Balancer requiere dos subredes que puedan enrutarse:

- Red de administración. La red de administración es donde reside la controladora de NSX Advanced Load Balancer, también denominada "Controladora". La red de administración proporciona al controlador conectividad con vCenter Server, hosts ESXi y nodos del plano de control del Supervisor. Esta red es donde se pone la interfaz de administración del motor de servicio de AVI. Esta red requiere un vDS y un grupo de puertos distribuidos.
- Red de datos. La interfaz de datos de los motores de servicio de AVI, también denominados motores de servicio, se conectan a esta red. Las direcciones IP virtuales (VIP) del equilibrador de carga se asignan desde esta red. Esta red requiere una instancia de VDS y grupos de puertos distribuidos. Debe configurar el vDS y los grupos de puertos distribuidos antes de instalar el equilibrador de carga.

Asignación de direcciones IP

El controlador y el motor de servicios se conectan a la red de administración. Al instalar y configurar NSX Advanced Load Balancer, proporcione una dirección IP estática y enrutable para cada máquina virtual del controlador.

Los motores de servicio pueden utilizar DHCP. Si DHCP no está disponible, puede configurar un grupo de direcciones IP para los motores de servicio.

Requisitos informáticos mínimos

En la tabla se especifican los requisitos informáticos mínimos para las redes VDS con NSX Advanced Load Balancer. Considere la posibilidad de separar el dominio de administración y el de carga de trabajo como práctica recomendada. El dominio de carga de trabajo aloja el Supervisor donde se ejecutan las cargas de trabajo. El dominio de administración aloja todos los componentes de administración, como vCenter Server.

Tabla 6-1. Requisitos informáticos mínimos

Sistema	Tamaño de implementación mínimo	CPU	Memoria	Almacenamiento
vCenter Server 8.0	Pequeño	2	21 GB	290 GB
Hosts ESXi 8.0	■ Sin vSAN: 3 hosts ESXi con 1 dirección IP estática por host. ■ Con vSAN: 4 hosts ESXi por clúster con al menos 2 NIC físicas. Los hosts deben unirse a un clúster con vSphere DRS y HA habilitados. vSphere DRS debe estar en el modo Totalmente automatizado o Parcialmente automatizado. **Nota** Asegúrese de que los nombres de los hosts que se unen al clúster utilicen letras minúsculas. De lo contrario, se puede producir un error en la habilitación del Supervisor.	8	64 GB por host	No aplicable
Máquinas virtuales de plano de control de Kubernetes	3	4	16 GB	16 GB
Controladora de NSX Advanced Load Balancer	Enterprise Para los entornos de producción, se recomienda instalar un clúster de 3 máquinas virtuales del Controlador AVI. Se requiere un mínimo de 2 máquinas virtuales del motor de servicio para HA.	4 (Pequeño) 8 (Medio) 24 (Grande)	12 GB 24 GB 128 GB	128 GB 128 GB 128 GB
Motor de servicio	Se requiere un mínimo de 2 máquinas virtuales del motor de servicio para HA.	1	2 GB	15 GB

Requisitos mínimos de red

En la tabla se especifican los requisitos de red mínimos para las redes de vSphere con NSX Advanced Load Balancer.

Nota No puede crear clústeres IPv6 con un Supervisor de vSphere 7 ni registrar clústeres IPv6 con Tanzu Mission Control. Actualmente, los servicios de NSX Advanced Load Balancer no admiten IPv6.

Tabla 6-2. Requisitos de red física

Componente	Cantidad mínima	Configuración necesaria
MTU de red física	1.500	El tamaño de MTU debe ser 1500 o superior en cualquier grupo de puertos distribuidos.

Tabla 6-3. Requisitos de red generales

Componente	Cantidad mínima	Configuración necesaria
Servidor NTP y DNS	1	Un servidor DNS y un servidor NTP que se pueden utilizar con vCenter Server. **Nota** Configure NTP en todos los hosts ESXi y vCenter Server.
servidor DHCP	1	Opcional. Configure un servidor DHCP para adquirir automáticamente direcciones IP para las redes de cargas de trabajo y administración, así como direcciones IP flotantes. El servidor DHCP debe admitir identificadores de cliente y proporcionar servidores DNS compatibles, dominios de búsqueda de DNS y un servidor NTP. Para la red de administración, todas las direcciones IP, como las direcciones IP de las máquinas virtuales del plano de control, una IP flotante, servidores DNS, DNS, dominios de búsqueda y servidor NTP, se adquieren automáticamente desde el servidor DHCP. Supervisor utiliza la configuración de DHCP. Los equilibradores de carga pueden requerir direcciones IP estáticas para la administración. Los ámbitos de DHCP no deben superponerse a estas direcciones IP estáticas. DHCP no se utiliza para direcciones IP virtuales. (VIP) **Nota** La configuración de DHCP para redes de cargas de trabajo no es compatible con servicios de supervisor en un Supervisor configurado con la pila de VDS. Para utilizar servicios de supervisor, configure redes de carga de trabajo con direcciones IP estáticas. Puede seguir utilizando DHCP para la red de administración.

Tabla 6-4. Requisitos de la red de administración

Componente	Cantidad mínima	Configuración necesaria
IP estáticas para las máquinas virtuales del plano de control de Kubernetes	Bloque de 5	Un bloque de 5 direcciones IP estáticas consecutivas que se asignarán desde la red de administración a las máquinas virtuales del plano de control de Kubernetes en el Supervisor.
Red de tráfico de administración	1	Una red de administración que se puede enrutar a los hosts ESXi, a vCenter Server, a la instancia de Supervisor y a un equilibrador de carga.
Subred de red de administración	1	La red de administración es donde reside la controladora de NSX Advanced Load Balancer, también denominada "Controladora". También es donde se conecta la interfaz de administración del motor de servicio. La controladora debe conectarse a las direcciones IP de administración de vCenter Server y ESXi desde esta red **Nota** La red de administración y la red de carga de trabajo deben estar en subredes diferentes. No se admite la asignación de la misma subred a las redes de administración y carga de trabajo, lo que puede provocar errores y problemas en el sistema.

Tabla 6-5. Requisitos de red de cargas de trabajo

Componente	Cantidad mínima	Configuración necesaria
vSphere Distributed Switch	1	Todos los hosts del clúster de vSphere deben estar conectados a una instancia de VDS.
Redes de cargas de trabajo	1	Se debe crear al menos un grupo de puertos distribuidos en la instancia de VDS que se configure como red de cargas de trabajo principal. Según la topología que elija, podrá utilizar el mismo grupo de puertos distribuidos como red de cargas de trabajo de los espacios de nombres o bien podrá crear más grupos de puertos y configurarlos como redes de cargas de trabajo. Las redes de cargas de trabajo deben cumplir los siguientes requisitos: ■ La función de enrutamiento entre las redes de cargas de trabajo con la red que utiliza NSX Advanced Load Balancer para la asignación de direcciones IP virtuales. ■ No hay superposición de los rangos de direcciones IP en todas las redes de cargas de trabajo dentro de Supervisor.
Rango de CIDR de servicios de Kubernetes	/16 direcciones IP privadas	Un rango de CIDR privado para asignar direcciones IP a los servicios de Kubernetes. Debe especificar un rango de CIDR único de servicios de Kubernetes para cada Supervisor.

Tabla 6-6. Requisitos de red del equilibrador de carga

Servidor NTP y DNS	1	La IP del servidor DNS es necesaria para que la controladora de NSX Advanced Load Balancer resuelva correctamente los nombres de host de vCenter Server y ESXi. NTP es opcional, ya que los servidores NTP públicos se utilizan de forma predeterminada.
Subred de red de datos	1	La interfaz de datos de los motores de servicio de NSX Advanced Load Balancer, también denominados "motores de servicio", se conecta a esta red. Configure un grupo de direcciones IP para los motores de servicio. Las direcciones IP virtuales (VIP) del equilibrador de carga se asignan desde esta red.
IP de la controladora de NSX Advanced Load Balancer	1 o 4	Si implementa la controladora de NSX Advanced Load Balancer como un solo nodo, se requiere una dirección IP estática para su interfaz de administración. Para un clúster de 3 nodos, se requieren 4 direcciones IP . Una para cada máquina virtual de la controladora de NSX Advanced Load Balancer y otra para la VIP del clúster. Estas direcciones IP deben proceder de la subred de la red de administración.
Rango de VIP de IPAM	-	Un rango de CIDR privado para asignar direcciones IP a los servicios de Kubernetes. Las direcciones IP deben proceder de la subred de la red de datos. Debe especificar un rango de CIDR de servicios de Kubernetes único para cada clúster supervisor.

Puertos y protocolos

En esta tabla se especifican los protocolos y los puertos necesarios para administrar la conectividad IP entre NSX Advanced Load Balancer, vCenter y otros componentes de vSphere IaaS control plane .

Origen	Destino	Protocolo y puertos
Controladora de NSX Advanced Load Balancer	Controladora de NSX Advanced Load Balancer (en el clúster)	TCP 22 (SSH) TCP 443 (HTTPS) TCP 8443 (HTTPS)
Motor de servicio	Engine de servicio en HA	TCP 9001 para VMware, LSC y NSX-T Cloud
Motor de servicio	Controladora de NSX Advanced Load Balancer	TCP 22 (SSH) TCP 8443 (HTTPS) TCP 123 (NTP)
Controlador AVI	vCenter Server, ESXi, NSX-T Manager	TCP 443 (HTTPS)
Nodos del plano de control de supervisor (AKO)	Controladora de NSX Advanced Load Balancer	TCP 443 (HTTPS)

Para obtener más información sobre los puertos y los protocolos de NSX Advanced Load Balancer, consulte https://ports.esp.vmware.com/home/NSX-Advanced-Load-Balancer.

Requisitos para la implementación de clústeres de Supervisor con NSX

Revise los requisitos del sistema para configurar vSphere IaaS control plane en un clúster de vSphere mediante el uso de la pilas de redes de NSX. Cuando se habilita un clúster de vSphere como Supervisor, se crea automáticamente una zona de vSphere para el Supervisor.

Además de estos requisitos, consulte la Guía de diseño de referencia de NSX para obtener más información sobre las prácticas recomendadas para implementar NSX.

Requisitos informáticos mínimos para el clúster de Edge y administración

Sistema	Tamaño de implementación mínimo	CPU	Memoria	Almacenamiento
vCenter Server 8	Pequeño	2	21 GB	290 GB
8 hosts ESXi	2 hosts ESXi	8	64 GB por host	No aplicable
NSX Manager	Mediano	6	24 GB	300 GB
NSX Edge 1	Grande	8	32 GB	200 GB
NSX Edge 2	Grande	8	32 GB	200 GB

Nota Compruebe que todos los hosts ESXi que participan en el clúster de vSphere en el que tiene pensado configurar vSphere IaaS control plane estén preparados como nodos de transporte de NSX. Para obtener más información, consulte https://kb.vmware.com/s/article/95820 y Preparar hosts ESXi como nodos de transporte en la documentación de NSX.

Requisitos informáticos mínimos para el clúster de dominio de carga de trabajo

Sistema	Tamaño de implementación mínimo	CPU	Memoria	Almacenamiento
Clústeres de vSphere	■ 1 clúster de vSphere ■ vSphere DRS y HA habilitados en cada clúster de vSphere. vSphere DRS debe estar en el modo Totalmente automatizado.	No aplicable	No aplicable	No aplicable
8 hosts ESXi	■ Sin vSAN: 3 hosts ESXi con 1 dirección IP estática por host. ■ Con vSAN: 4 hosts ESXi con al menos 2 NIC físicas. **Nota** Asegúrese de que los nombres de los hosts que se unen a los clústeres utilicen letras minúsculas. De lo contrario, se puede producir un error en la activación del Supervisor.	8	64 GB por host	No aplicable
Máquinas virtuales de plano de control de Kubernetes	3	4	16 GB	16 GB

Requisitos de red

Nota No puede crear clústeres IPv6 con un Supervisor de vSphere 8 ni registrar clústeres IPv6 con Tanzu Mission Control.

Compruebe la Matriz de interoperabilidad de productos VMware para conocer las versiones de NSX compatibles.

Tabla 6-7. Requisitos de red física

Componente	Cantidad mínima	Configuración necesaria
MTU de red física	1.500	El tamaño de MTU debe ser 1500 o superior en cualquier grupo de puertos de vSphere Distributed Switch.
NIC física	Al menos 2 NIC físicas por host si se utiliza vSAN	Para utilizar la CNI de Antrea y obtener un rendimiento de NSX óptimo, cada NIC física en cada host ESXi participante debe admitir la encapsulación GENEVE y debe tenerla habilitada.

Tabla 6-8. Requisitos de red generales

Componente	Cantidad mínima	Configuración necesaria
Servidor NTP y DNS	1	Un servidor DNS y un servidor NTP que se pueden utilizar con vCenter Server. **Nota** Configure NTP en todos los hosts ESXi y vCenter Server.
servidor DHCP	1	Opcional. Configure un servidor DHCP para adquirir automáticamente direcciones IP para las redes de administración y cargas de trabajo, así como direcciones IP flotantes. El servidor DHCP debe admitir identificadores de cliente y proporcionar servidores DNS compatibles, dominios de búsqueda de DNS y un servidor NTP. Para la red de administración, todas las direcciones IP, como las direcciones IP de las máquinas virtuales del plano de control, una IP flotante, servidores DNS, DNS, dominios de búsqueda y servidor NTP, se adquieren automáticamente desde el servidor DHCP. Supervisor utiliza la configuración de DHCP. Los equilibradores de carga pueden requerir direcciones IP estáticas para la administración. Los ámbitos de DHCP no deben superponerse a estas direcciones IP estáticas. DHCP no se utiliza para direcciones IP virtuales. (VIP)
Registro de imágenes	1	Acceda a un registro para el servicio.

Tabla 6-9. Requisitos de la red de administración

Componente	Cantidad mínima	Configuración necesaria
IP estáticas para las máquinas virtuales del plano de control de Kubernetes	Bloque de 5	Un bloque de 5 direcciones IP estáticas consecutivas que se asignarán desde la red de administración a las máquinas virtuales del plano de control de Kubernetes en el Supervisor.
Red de tráfico de administración	1	Una red de administración que se puede enrutar a los hosts ESXi, a vCenter Server, a la instancia de Supervisor y a un equilibrador de carga.
Subred de red de administración	1	La subred que se utiliza para el tráfico de administración entre los hosts ESXi y vCenter Server, las instancias de NSX Appliance y el plano de control de Kubernetes. El tamaño de la subred debe ser el siguiente: ■ Una dirección IP por adaptador de VMkernel de host. ■ Una dirección IP para vCenter Server Appliance. ■ Una o cuatro direcciones IP para NSX Manager. Cuatro cuando se realiza una agrupación de NSX Manager de 3 nodos y 1 IP virtual (VIP). ■ 5 direcciones IP para el plano de control de Kubernetes. 1 para cada uno de los 3 nodos, 1 para la IP virtual, 1 para la actualización sucesiva de clústeres. **Nota** La red de administración y la red de carga de trabajo deben estar en subredes diferentes. No se admite la asignación de la misma subred a las redes de administración y carga de trabajo, lo que puede provocar errores y problemas en el sistema.
VLAN de red de administración	1	Identificador de VLAN de la subred de la red de administración.

Tabla 6-10. Requisitos de red de cargas de trabajo

Componente	Cantidad mínima	Configuración necesaria
Rango de CIDR del pod de vSphere	/23 direcciones IP privadas	Un rango de CIDR privado que proporciona direcciones IP a los pods de vSphere. Estas direcciones también se utilizan para los nodos del clúster de Tanzu Kubernetes Grid. Debe especificar un rango de CIDR único del pod de vSphere para cada clúster. **Nota** El rango de CIDR del pod de vSphere y el rango de CIDR de las direcciones del servicio de Kubernetes no deben superponerse.
Rango de CIDR de servicios de Kubernetes	/16 direcciones IP privadas	Un rango de CIDR privado para asignar direcciones IP a los servicios de Kubernetes. Debe especificar un rango de CIDR único de servicios de Kubernetes para cada Supervisor.
Rango de CIDR de salida	/27 direcciones IP estáticas	Una anotación de CIDR privado para determinar la IP de egreso de los servicios de Kubernetes. Solo se asigna una dirección IP de egreso para cada espacio de nombres en el Supervisor. La IP de egreso es la dirección que las entidades externas utilizan para comunicarse con los servicios en el espacio de nombres. La cantidad de direcciones IP de egreso limita el número de directivas de egreso que puede tener el Supervisor. El valor mínimo es un CIDR de /27 o más. Por ejemplo, `10.174.4.96/27` **Nota** Las direcciones IP de egreso y las direcciones IP de entrada no deben superponerse.

Tabla 6-10. Requisitos de red de cargas de trabajo (continuación)

Componente	Cantidad mínima	Configuración necesaria
CIDR de entrada	/27 direcciones IP estáticas	Un rango de CIDR privado que se utilizará para las direcciones IP de entradas. La entrada permite aplicar directivas de tráfico a las solicitudes que entran en Supervisor desde redes externas. La cantidad de direcciones IP de entrada limita el número de entradas que puede tener el clúster. El valor mínimo es un CIDR de /27 o más. **Nota** Las direcciones IP de egreso y las direcciones IP de entrada no deben superponerse.
Rango de redes de espacio de nombres	1	Uno o varios CIDR de IP para crear subredes o segmentos y asignar direcciones IP a las cargas de trabajo.
Prefijo de subred de espacio de nombres	1	El prefijo de subred que especifica el tamaño de la subred reservada para segmentos de espacios de nombres. El valor predeterminado es 28.

Tabla 6-11. Requisitos de NSX

Componente	Cantidad mínima	Configuración necesaria
VLAN	3	Las IP de VLAN son las direcciones IP de los endpoints de túnel (Tunnel Endpoints, TEP). Los TEP del host ESXi y los TEP de Edge deben ser enrutables. Las direcciones IP de VLAN son necesarias para lo siguiente: ■ VTEP de host ESXi ■ VTEP de Edge con la IP estática ■ Puerta de enlace de nivel 0 y vínculo superior para el nodo de transporte. **Nota** El VTEP del host ESXi y el VTEP de Edge deben tener un tamaño de MTU superior a 1600. Los hosts ESXi y los nodos de NSX-T Edge actúan como endpoints de túnel y se asigna una IP de endpoint de túnel (Tunnel Endpoint, TEP) a cada nodo de Edge y host. Como las IP de TEP para hosts ESXi crean un túnel de superposición con IP de TEP en los nodos de Edge, las IP de VLAN deben poder enrutarse. Se requiere una VLAN adicional para proporcionar conectividad de norte a sur a la puerta de enlace de nivel 0. Los grupos de direcciones IP pueden compartirse entre clústeres. Sin embargo, el grupo de direcciones IP/VLAN de superposición de host no se debe compartir con la VLAN o el grupo de direcciones IP de superposición de Edge. **Nota** Si el TEP del host y el TEP de Edge usan diferentes NIC físicas, pueden utilizar la misma VLAN.
IP de vínculo superior de nivel 0	/24 direcciones IP privadas	La subred de IP que se utiliza para el vínculo superior de nivel 0. Los requisitos para la dirección IP del vínculo superior de nivel 0 son los siguientes: ■ 1 dirección IP, si no se requiere redundancia de Edge. ■ 4 direcciones IP; si utiliza BGP y redundancia de Edge, necesitará 2 direcciones IP por Edge. ■ 3 direcciones IP, si utiliza rutas estáticas y redundancia de Edge. La IP de administración de Edge, la subred, la puerta de enlace, la IP de vínculo superior, la subred y la puerta de enlace deben ser únicas.

Requisitos para la implementación de Supervisor del clúster con NSX y NSX Advanced Load Balancer

Revise los requisitos del sistema para configurar vSphere IaaS control plane en un clúster de vSphere mediante el uso de la pilas de redes de NSX. Cuando se habilita un clúster de vSphere como Supervisor, se crea automáticamente una zona de vSphere para el Supervisor.

Opciones de implementación de NSX

Para obtener más información sobre las prácticas recomendadas para implementar NSX, consulte Guía de diseño de referencia de NSX.

Requisitos informáticos mínimos para el clúster de Edge y administración

Sistema	Tamaño de implementación mínimo	CPU	Memoria	Almacenamiento
vCenter Server 8	Pequeño	2	21 GB	290 GB
8 hosts ESXi	2 hosts ESXi	8	64 GB por host	No aplicable
NSX Manager	Mediano	6	24 GB	300 GB
NSX Edge 1	Grande	8	32 GB	200 GB
NSX Edge 2	Grande	8	32 GB	200 GB
Máquinas virtuales del motor de servicio	Se implementan al menos dos máquinas virtuales del motor de servicio por Supervisor	1	2 GB	N/C

Nota Compruebe que todos los hosts ESXi que participan en el clúster de vSphere en el que tiene pensado configurar vSphere IaaS control plane estén preparados como nodos de transporte de NSX. Para obtener más información, consulte https://kb.vmware.com/s/article/95820 y Preparar hosts ESXi como nodos de transporte en la documentación de NSX.

Especificar la capacidad del sistema del controlador

Puede especificar la capacidad del sistema del controlador durante la implementación. La capacidad del sistema se basa en asignaciones de recursos del sistema, como CPU, RAM y disco. La cantidad de recursos que asigne tiene un impacto en el rendimiento del controlador.

Tipo de implementación	Recuento de nodos	Asignaciones recomendadas: CPU	Asignaciones recomendadas: memoria	Asignaciones recomendadas: disco
Demostración/ Evaluación del cliente	1	6	24 GB	128 GB

En las implementaciones de demostración, con un único controlador es suficiente y se utiliza para todas las actividades y los flujos de trabajo del plano de control, así como para los análisis.

En una implementación de producción, se recomienda un clúster de tres nodos.

Para obtener más información, consulte Tamaño del controlador de NSX Advanced Load Balancer.

Requisitos informáticos mínimos para el clúster de dominio de carga de trabajo

Sistema	Tamaño de implementación mínimo	CPU	Memoria	Almacenamiento
Clústeres de vSphere	■ 1 clúster de vSphere ■ vSphere DRS y HA habilitados en cada clúster de vSphere. vSphere DRS debe estar en el modo Totalmente automatizado.	No aplicable	No aplicable	No aplicable
8 hosts ESXi	■ Sin vSAN: 3 hosts ESXi con 1 dirección IP estática por host. ■ Con vSAN: 4 hosts ESXi con al menos 2 NIC físicas. **Nota** Asegúrese de que los nombres de los hosts que se unen a los clústeres utilicen letras minúsculas. De lo contrario, se puede producir un error en la activación del Supervisor.	8	64 GB por host	No aplicable
Máquinas virtuales de plano de control de Kubernetes	3	4	16 GB	16 GB

Requisitos de red

Nota No puede crear clústeres IPv6 con un Supervisor de vSphere 8 ni registrar clústeres IPv6 con Tanzu Mission Control.

Compruebe la Matriz de interoperabilidad de productos VMware para conocer las versiones de NSX compatibles.

Tabla 6-12. Requisitos de red física

Componente	Cantidad mínima	Configuración necesaria
MTU de red física	1700	El tamaño de MTU debe ser 1700 o superior en cualquier grupo de puertos de vSphere Distributed Switch.
NIC física	Al menos 2 NIC físicas por host si se utiliza vSAN	Para utilizar la CNI de Antrea y obtener un rendimiento de NSX óptimo, cada NIC física en cada host ESXi participante debe admitir la encapsulación GENEVE y debe tenerla habilitada.

Tabla 6-13. Requisitos de red generales

Componente	Cantidad mínima	Configuración necesaria
Servidor NTP y DNS	1	Un servidor DNS y un servidor NTP que se pueden utilizar con vCenter Server. **Nota** Configure NTP en todos los hosts ESXi y vCenter Server.
servidor DHCP	1	Opcional. Configure un servidor DHCP para adquirir automáticamente direcciones IP para las redes de administración y cargas de trabajo, así como direcciones IP flotantes. El servidor DHCP debe admitir identificadores de cliente y proporcionar servidores DNS compatibles, dominios de búsqueda de DNS y un servidor NTP. Para la red de administración, todas las direcciones IP, como las direcciones IP de las máquinas virtuales del plano de control, una IP flotante, servidores DNS, DNS, dominios de búsqueda y servidor NTP, se adquieren automáticamente desde el servidor DHCP. Supervisor utiliza la configuración de DHCP. Los equilibradores de carga pueden requerir direcciones IP estáticas para la administración. Los ámbitos de DHCP no deben superponerse a estas direcciones IP estáticas. DHCP no se utiliza para direcciones IP virtuales. (VIP)
Registro de imágenes	1	Acceda a un registro para el servicio.

Tabla 6-14. Requisitos de la red de administración

Componente	Cantidad mínima	Configuración necesaria
IP estáticas para las máquinas virtuales del plano de control de Kubernetes	Bloque de 5	Un bloque de 5 direcciones IP estáticas consecutivas que se asignarán desde la red de administración a las máquinas virtuales del plano de control de Kubernetes en el Supervisor.
Red de tráfico de administración	1	Una red de administración que se puede enrutar a los hosts ESXi, a vCenter Server, a la instancia de Supervisor y a un equilibrador de carga.
Subred de red de administración	1	La subred que se utiliza para el tráfico de administración entre los hosts ESXi y vCenter Server, las instancias de NSX Appliance y el plano de control de Kubernetes. El tamaño de la subred debe ser el siguiente: ■ Una dirección IP por adaptador de VMkernel de host. ■ Una dirección IP para vCenter Server Appliance. ■ Una o cuatro direcciones IP para NSX Manager. Cuatro cuando se realiza una agrupación de NSX Manager de 3 nodos y 1 IP virtual (VIP). ■ 5 direcciones IP para el plano de control de Kubernetes. 1 para cada uno de los 3 nodos, 1 para la IP virtual, 1 para la actualización sucesiva de clústeres. **Nota** La red de administración y la red de carga de trabajo deben estar en subredes diferentes. No se admite la asignación de la misma subred a las redes de administración y carga de trabajo, lo que puede provocar errores y problemas en el sistema.
VLAN de red de administración	1	Identificador de VLAN de la subred de la red de administración.

Tabla 6-15. Requisitos de red de cargas de trabajo

Componente	Cantidad mínima	Configuración necesaria
Rango de CIDR del pod de vSphere	/23 direcciones IP privadas	Un rango de CIDR privado que proporciona direcciones IP a los pods de vSphere. Estas direcciones también se utilizan para los nodos del clúster de Tanzu Kubernetes Grid. Debe especificar un rango de CIDR único del pod de vSphere para cada clúster. **Nota** El rango de CIDR del pod de vSphere y el rango de CIDR de las direcciones del servicio de Kubernetes no deben superponerse.
Rango de CIDR de servicios de Kubernetes	/16 direcciones IP privadas	Un rango de CIDR privado para asignar direcciones IP a los servicios de Kubernetes. Debe especificar un rango de CIDR único de servicios de Kubernetes para cada Supervisor.
Rango de CIDR de salida	/27 direcciones IP estáticas	Una anotación de CIDR privado para determinar la IP de egreso de los servicios de Kubernetes. Solo se asigna una dirección IP de egreso para cada espacio de nombres en el Supervisor. La IP de egreso es la dirección que las entidades externas utilizan para comunicarse con los servicios en el espacio de nombres. La cantidad de direcciones IP de egreso limita el número de directivas de egreso que puede tener el Supervisor. El valor mínimo es un CIDR de /27 o más. Por ejemplo, `10.174.4.96/27` **Nota** Las direcciones IP de egreso y las direcciones IP de entrada no deben superponerse.

Tabla 6-15. Requisitos de red de cargas de trabajo (continuación)

Componente	Cantidad mínima	Configuración necesaria
CIDR de entrada	/27 direcciones IP estáticas	Un rango de CIDR privado que se utilizará para las direcciones IP de entradas. La entrada permite aplicar directivas de tráfico a las solicitudes que entran en Supervisor desde redes externas. La cantidad de direcciones IP de entrada limita el número de entradas que puede tener el clúster. El valor mínimo es un CIDR de /27 o más. **Nota** Las direcciones IP de egreso y las direcciones IP de entrada no deben superponerse.
Rango de redes de espacio de nombres	1	Uno o varios CIDR de IP para crear subredes o segmentos y asignar direcciones IP a las cargas de trabajo.
Prefijo de subred de espacio de nombres	1	El prefijo de subred que especifica el tamaño de la subred reservada para segmentos de espacios de nombres. El valor predeterminado es 28.

Tabla 6-16. Requisitos de NSX

Componente	Cantidad mínima	Configuración necesaria
VLAN	3	Las IP de VLAN son las direcciones IP de los endpoints de túnel (Tunnel Endpoints, TEP). Los TEP del host ESXi y los TEP de Edge deben ser enrutables. Las direcciones IP de VLAN son necesarias para lo siguiente: ■ VTEP de host ESXi ■ VTEP de Edge con la IP estática ■ Puerta de enlace de nivel 0 y vínculo superior para el nodo de transporte. **Nota** El VTEP del host ESXi y el VTEP de Edge deben tener un tamaño de MTU superior a 1600. Los hosts ESXi y los nodos de NSX-T Edge actúan como endpoints de túnel y se asigna una IP de endpoint de túnel (Tunnel Endpoint, TEP) a cada nodo de Edge y host. Como las IP de TEP para hosts ESXi crean un túnel de superposición con IP de TEP en los nodos de Edge, las IP de VLAN deben poder enrutarse. Se requiere una VLAN adicional para proporcionar conectividad de norte a sur a la puerta de enlace de nivel 0. Los grupos de direcciones IP pueden compartirse entre clústeres. Sin embargo, el grupo de direcciones IP/VLAN de superposición de host no se debe compartir con la VLAN o el grupo de direcciones IP de superposición de Edge. **Nota** Si el TEP del host y el TEP de Edge usan diferentes NIC físicas, pueden utilizar la misma VLAN.
IP de vínculo superior de nivel 0	/24 direcciones IP privadas	La subred de IP que se utiliza para el vínculo superior de nivel 0. Los requisitos para la dirección IP del vínculo superior de nivel 0 son los siguientes: ■ 1 dirección IP, si no se requiere redundancia de Edge. ■ 4 direcciones IP; si utiliza BGP y redundancia de Edge, necesitará 2 direcciones IP por Edge. ■ 3 direcciones IP, si utiliza rutas estáticas y redundancia de Edge. La IP de administración de Edge, la subred, la puerta de enlace, la IP de vínculo superior, la subred y la puerta de enlace deben ser únicas.

Tabla 6-17. Requisitos de red del equilibrador de carga

Servidor NTP y DNS	1	La IP del servidor DNS es necesaria para que la controladora de NSX Advanced Load Balancer resuelva correctamente los nombres de host de vCenter Server y ESXi. NTP es opcional, ya que los servidores NTP públicos se utilizan de forma predeterminada.
Subred de red de datos	1	La interfaz de datos de los motores de servicio de NSX Advanced Load Balancer, también denominados "motores de servicio", se conecta a esta red. Configure un grupo de direcciones IP para los motores de servicio. Las direcciones IP virtuales (VIP) del equilibrador de carga se asignan desde esta red.
IP de la controladora de NSX Advanced Load Balancer	1 o 4	Si implementa la controladora de NSX Advanced Load Balancer como un solo nodo, se requiere una dirección IP estática para su interfaz de administración. Para un clúster de 3 nodos, se requieren 4 direcciones IP . Una para cada máquina virtual de la controladora de NSX Advanced Load Balancer y otra para la VIP del clúster. Estas direcciones IP deben proceder de la subred de la red de administración.
Rango de VIP de IPAM	-	Un rango de CIDR privado para asignar direcciones IP a los servicios de Kubernetes. Las direcciones IP deben proceder de la subred de la red de datos. Debe especificar un rango de CIDR de servicios de Kubernetes único para cada clúster supervisor.

Puertos y protocolos

En esta tabla se especifican los protocolos y los puertos necesarios para administrar la conectividad IP entre NSX Advanced Load Balancer, vCenter y otros componentes de vSphere IaaS control plane .

Origen	Destino	Protocolo y puertos
Controladora de NSX Advanced Load Balancer	Controladora de NSX Advanced Load Balancer (en el clúster)	TCP 22 (SSH) TCP 443 (HTTPS) TCP 8443 (HTTPS)
Motor de servicio	Engine de servicio en HA	TCP 9001 para VMware, LSC y NSX-T Cloud
Motor de servicio	Controladora de NSX Advanced Load Balancer	TCP 22 (SSH) TCP 8443 (HTTPS) TCP 123 (NTP)
Controlador AVI	vCenter Server, ESXi, NSX-T Manager	TCP 443 (HTTPS)
Nodos del plano de control de supervisor (AKO)	Controladora de NSX Advanced Load Balancer	TCP 443 (HTTPS)

Para obtener más información sobre los puertos y los protocolos de NSX Advanced Load Balancer, consulte https://ports.esp.vmware.com/home/NSX-Advanced-Load-Balancer.

Requisitos para la implementación de clústeres de Supervisor con redes VDS y equilibrador de carga de HAProxy

Compruebe los requisitos del sistema para configurar un clúster de vSphere como un Supervisor con la pila de redes VDS y el equilibrador de carga de HAProxy. Cuando se habilita un clúster de vSphere como Supervisor, se crea automáticamente una zona de vSphere para el Supervisor.

Requisitos informáticos mínimos

Considere la posibilidad de separar el dominio de administración y el de carga de trabajo como práctica recomendada. El dominio de carga de trabajo aloja el Supervisor donde se ejecutan las cargas de trabajo. El dominio de administración aloja todos los componentes de administración, como vCenter Server.

Sistema	Tamaño de implementación mínimo	CPU	Memoria	Almacenamiento
vCenter Server 8.0	Pequeño	2	21 GB	290 GB
Hosts ESXi 8.0	Sin vSAN: 3 hosts ESXi con 1 dirección IP estática por host. Con vSAN: 4 hosts ESXi con al menos 2 NIC físicas. Los hosts deben unirse a un clúster con vSphere DRS y HA habilitados. vSphere DRS debe estar en el modo Totalmente automatizado o Parcialmente automatizado. **Nota** Asegúrese de que los nombres de los hosts que se unen al clúster utilicen letras minúsculas. De lo contrario, se puede producir un error en la habilitación del clúster para la administración de cargas de trabajo.	8	64 GB por host	No aplicable
Máquinas virtuales de plano de control de Kubernetes	3	4	16 GB	16 GB

Requisitos mínimos de red

Nota No puede crear clústeres IPv6 con un Supervisor de vSphere 8 ni registrar clústeres IPv6 con Tanzu Mission Control.

Tabla 6-18. Requisitos de red física

Componente	Cantidad mínima	Configuración necesaria
MTU de red física	1.500	El tamaño de MTU debe ser 1500 o superior en cualquier grupo de puertos distribuidos.

Tabla 6-19. Requisitos de red generales

Componente	Cantidad mínima	Configuración necesaria
Servidor NTP y DNS	1	Un servidor DNS y un servidor NTP que se pueden utilizar con vCenter Server. **Nota** Configure NTP en todos los hosts ESXi y vCenter Server.
servidor DHCP	1	Opcional. Configure un servidor DHCP para adquirir automáticamente direcciones IP para las redes de administración y cargas de trabajo, así como direcciones IP flotantes. El servidor DHCP debe admitir identificadores de cliente y proporcionar servidores DNS compatibles, dominios de búsqueda de DNS y un servidor NTP. Para la red de administración, todas las direcciones IP, como las direcciones IP de las máquinas virtuales del plano de control, una IP flotante, servidores DNS, DNS, dominios de búsqueda y servidor NTP, se adquieren automáticamente desde el servidor DHCP. Supervisor utiliza la configuración de DHCP. Los equilibradores de carga pueden requerir direcciones IP estáticas para la administración. Los ámbitos de DHCP no deben superponerse a estas direcciones IP estáticas. DHCP no se utiliza para direcciones IP virtuales. (VIP) **Nota** La configuración de DHCP para redes de cargas de trabajo no es compatible con servicios de supervisor en un Supervisor configurado con la pila de VDS. Para utilizar servicios de supervisor, configure redes de carga de trabajo con direcciones IP estáticas. Puede seguir utilizando DHCP para la red de administración.

Tabla 6-20. Requisitos de la red de administración

Componente	Cantidad mínima	Configuración necesaria
IP estáticas para las máquinas virtuales del plano de control de Kubernetes	Bloque de 5	Un bloque de 5 direcciones IP estáticas consecutivas que se asignarán desde la red de administración a las máquinas virtuales del plano de control de Kubernetes en el Supervisor.
Red de tráfico de administración	1	Una red de administración que se puede enrutar a los hosts ESXi, a vCenter Server, a la instancia de Supervisor y a un equilibrador de carga.

Tabla 6-20. Requisitos de la red de administración (continuación)

Componente	Cantidad mínima	Configuración necesaria
Subred de red de administración	1	La subred que se utiliza para el tráfico de administración entre los hosts ESXi y vCenter Server y el plano de control de Kubernetes. El tamaño de la subred debe ser el siguiente: ■ Una dirección IP por adaptador de VMkernel de host. ■ Una dirección IP para vCenter Server Appliance. ■ 5 direcciones IP para el plano de control de Kubernetes. 1 para cada uno de los 3 nodos, 1 para la IP virtual, 1 para la actualización sucesiva de clústeres. **Nota** La red de administración y la red de carga de trabajo deben estar en subredes diferentes. No se admite la asignación de la misma subred a las redes de administración y carga de trabajo, lo que puede provocar errores y problemas en el sistema.
VLAN de red de administración	1	Identificador de VLAN de la subred de la red de administración.

Tabla 6-21. Requisitos de red de cargas de trabajo

Componente	Cantidad mínima	Configuración necesaria
vSphere Distributed Switch	1	Todos los hosts del clúster de vSphere deben estar conectados a una instancia de VDS.
Redes de cargas de trabajo	1	Se debe crear al menos un grupo de puertos distribuidos en la instancia de VDS que se configure como red de cargas de trabajo principal. Según la topología que elija, podrá utilizar el mismo grupo de puertos distribuidos como red de cargas de trabajo de los espacios de nombres o bien podrá crear más grupos de puertos y configurarlos como redes de cargas de trabajo. Las redes de cargas de trabajo deben cumplir los siguientes requisitos: ■ La función de enrutamiento entre las redes de cargas de trabajo con la red que utiliza HAProxy para la asignación de direcciones IP virtuales. ■ No hay superposición de los rangos de direcciones IP en todas las redes de cargas de trabajo dentro de Supervisor. **Importante** La red de carga de trabajo debe estar en una subred diferente a la red de administración.
Rango de CIDR de servicios de Kubernetes	/16 direcciones IP privadas	Un rango de CIDR privado para asignar direcciones IP a los servicios de Kubernetes. Debe especificar un rango de CIDR único de servicios de Kubernetes para cada Supervisor.

Tabla 6-22. Requisitos de red del equilibrador de carga

Equilibrador de carga de HAProxy	1	Una instancia del equilibrador de carga de HAProxy configurada con la instancia de vCenter Server. ■ Si la misma instancia de HAProxy atiende a varios Supervisores debe poder enrutar el tráfico que se dirige a todas las redes de cargas de trabajo y el tráfico que procede de ellas en todos los Supervisores. ■ Los rangos de direcciones IP en las redes de cargas de trabajo en todos los Supervisores a los que atiende HAProxy no deben superponerse. ■ La red que utiliza HAProxy para asignar direcciones IP virtuales debe enrutarse a las redes de cargas de trabajo que se utilizan en todos los Supervisores a los que se conecta HAProxy.
Rango de IP del servidor virtual	1	Un rango de IP dedicado para direcciones IP virtuales. La máquina virtual de HAProxy debe ser el único propietario de este rango de IP virtual. El rango no debe superponerse con ningún otro rango de IP asignado a alguna red de cargas de trabajo que sea propiedad de una instancia de Supervisor. El rango no debe residir en la misma subred que la red de administración.

Componente	Cantidad mínima	Configuración necesaria
Servidor NTP y DNS	1	Un servidor DNS y un servidor NTP que se pueden utilizar con vCenter Server. **Nota** Configure NTP en todos los hosts ESXi y vCenter Server.
servidor DHCP	1	Opcional. Configure un servidor DHCP para adquirir automáticamente direcciones IP para las redes de administración y cargas de trabajo, así como direcciones IP flotantes. El servidor DHCP debe admitir identificadores de cliente y proporcionar servidores DNS compatibles, dominios de búsqueda de DNS y un servidor NTP. Supervisor utiliza la configuración de DHCP. Los equilibradores de carga pueden requerir direcciones IP estáticas para la administración. Los ámbitos de DHCP no deben superponerse a estas direcciones IP estáticas. DHCP no se utiliza para direcciones IP virtuales. (VIP)